Version: 2015-06-29

RCCMD – Multiple Server Shutdown Software

Benutzerhandbuch

Version: 2015-06-29

Urheberrechts-Erklärung zum geistigen Eigentum und Umgang mit vertraulichen Informationen

Die Informationen in diesem Benutzerhandbuch sind nicht bedingte Anweisungen und können ohne Ankündigung verändert werden. Obwohl GENEREX versucht hat, präzise Informationen in diesem Dokument bereitzustellen, übernimmt GENEREX keine Verantwortung für die Genauigkeit dieser Informationen.

GENEREX ist nicht verantwortlich für jeden indirekten, speziellen, daraus folgenden oder unbeabsichtigten Schaden, ohne Einschränkungen, verlorener Gewinne oder Einkommen, Kosten von Austausch Gütern, Verlust oder Beschädigung von Daten, die sich durch den Gebrauch dieses Dokumentes oder das hier beschriebenen Produkt ergeben.

GENEREX als Hersteller der genannten Produkte, übernimmt keine Verpflichtungen mit diesen Informationen. Die Produkte, die in diesem Handbuch beschrieben werden, wurden auf der alleinigen Basis von Informationen für Geschäftspartner gegeben, damit diese ein besseres Verständnis für die GENEREX Produkte erhalten.

GENEREX erlaubt seinen Geschäftspartnern die Informationen, die in diesem Dokument enthalten sind, an Dritte weiterzugeben, ebenso an das Personal in deren Firma oder ihren eigenen Kunden, elektronisch, manuell, in Form von Fotokopien oder Ähnlichem. GENEREX gibt an, dass der Inhalt nicht verändert oder angepasst werden darf, ohne schriftliche Genehmigung von GENEREX.

Alle Rechte, Titel und Interessen am GENEREX Markenzeichen BACS oder Firmenzeichen (registriert oder nicht registriert) oder der Geschäftswert bzw. das geistige Eigentum von GENEREX, das Urheberrecht und die Produkt-Patente sind exklusiv und ohne Einschränkungen im Eigentum von GENEREX.

GENEREX wird jede Beanstandung über den Inhalt dieses Dokumentes zeitnah abwickeln. Kommentare oder Beanstandungen zu diesem Dokument sollten an die GENEREX Systems Vertriebsgesellschaft mbH adressiert werden.

Das Urheberrecht der Europäischen Union ist gültig (Copyright EU).

Copyright (c) 1995-2015 GENEREX GmbH, Hamburg, Deutschland.

Alle Rechte vorbehalten.

Revision	History	Date
-001	Erstausgabe	10/2008
-012	Added: RCCMD auf XEN und ESX Server	12/2008
-013	RCCMD mit SSL	12/2008
-014	Update: UNIX multiple Sender Konfiguration	01/2009
-015	Added: Alternative SSL Konfiguration	02/2009
-016	Added: Syntax Schalten der Outputs	03/2009
-017	Added: RCCMD Relay auf UNIX	03/2009
-018	Update: Installation von RCCMD	06/2009
-019	Update: RCCMD Installation mit InstallAnywhere	07/2009
-020	Added: Silent Installation Windows	08/2009
-021	Added: Grafische RCCMD Relay Konfiguration Windows	08/2009
-022	Added: Kombi-Silent- und Konfigurations Installation	10/2009
-023	Added: RCCMD auf ESXi 4.0.x	10/2009
-024	Added: Silent Installation UNIX	11/2009
-025	Added: Console Installation UNIX	11/2009
-026	Added: Know How Pool	11/2009
-027	Added: Automatisches Zurücksetzen des Redundanz Alarms	01/2010
-028	Added: Grafische RCCMD Relay Konfiguration UNIX/MAC	03/2010
-029	Added: Configuration on Windows 2008 Server Core x64	07/2010
-030	Added: RCCMD FAQ	08/2010
-031	Added: RCCMD on ESXi 4.1 with vMA 4.1	11/2010
-032	Added: RCCMD Tray Beschreibung	06/2011
-033	Added: Raritan PDU Konfiguration	09/2011
-034	Added: RCCMD on ESXi 5	10/2011
-035	Added: RCCMD WebInterface	04/2012
-036	Added: RCCMD with VMware vCenter	08/2012
-037	Added: RCCMD Email Settings	08/2013
-038	Added: RCCMD Installation with vCenter	08/2014
-039	Updated: New RCCMD WebInterface Design	09/2014

Inhalt

1. Was ist die RCCMD Software? 5
1.1 Netzwerk Shutdown mit RCCMD 6
2. Installation / Konfiguration von RCCMD für Windows 7
2.1 Installation von RCCMD 8
2.1.1 Silent Installation für die RCCMD Installation 14
2.1.2 RCCMD Silent Installation mit Übernahme eigener Konfiguration 17
2.2 Console Installation für die RCCMD Installation 18
2.2.1 Beispiel einer Console Installation 18
2.2 RCCMD WebInterface (ab Version 4.0.1.9) 21
2.2.1 RCCMD WebInterface Remote Zugriff 33
2.3 Der RCCMD Client als Relay Station 34
2.4 Automatisches Zurücksetzen des Redundanz Alarms 35
2.5 RCCMD mit SSL auf Windows 37
2.5.1 RCCMD mit eigenen SSL Zertifikaten 39
2.6 Einstellungen der Berechtigung für den RCCMD Dienst 40
2.7 Testen des Shutdown.Bat Files 44
2.8 Testen der RCCMD Verbindung 46
2.8.1 Testen der RCCMD 2 Verbindung 46
2.9 RCCMD auf Windows 95/98 47
2.10 RCCMD auf Windows NT/2000/XP/2003/2008 48
2.11 RCCMD auf Windows 2008 Server Core x64 49
2.12 Alte RCCMD Konfiguration 50
2.12.1 Der RCCMD Client als Relay Station 56
3. RCCMD auf UNIX (mit grafischer Oberfläche) 60
3.1 RCCMD Installation auf UNIX OS 60
3.2 Silent Installation für die RCCMD Installation auf UNIX OS 67
3.3 Console Installation für die RCCMD Installation auf UNIX OS 69
3.3.1 Beispiel einer Console Installation 70
3.4 RCCMD WebInterface (ab Version 4.2.0.0) 73
3.5 RCCMD WebInterface Remote Zugriff 81
3.6 Automatisches Zurücksetzen des Redundanz Alarms 82
3.7 RCCMD mit SSL auf UNIX 83
3.7.1 RCCMD mit eigenen SSL Zertifikaten 86
3.8 Alternative RCCMD Konfiguration über Editor 86
3.9 Alte RCCMD Konfiguration auf UNIX OS 89
3.9.1 Der RCCMD Client als Relay Station 95
3.10 UNIX RCCMD Konfiguration mit CURSES Library 97

4. RCCMD auf VMware 110
4.1 RCCMD auf VMware ESX 110
4.2 RCCMD auf VMware ESXi 4.x – 5.x 111
4.2.1 ESXi Host Konfiguration über die vMA und vSphere 112
4.2.2 Shutdown Konfiguration virtuelle Maschinen auf dem ESXi 112
4.2.3 RCCMD Installation auf der vMA 115
4.2.3.1 RCCMD Installation ohne vCenter 118
4.2.3.2 RCCMD Installation mit vCenter 119
4.2.4 RCCMD WebInterface Konfiguration (ab Version 4.2.0.0) 123
4.2.4.1 RCCMD WebInterface mit vCenter 129
4.2.5 RCCMD Installation auf der vMA 6 (ab RCCMD V 4.3.0.2) 134
4.2.5.1 RCCMD Installation ohne vCenter 137
4.2.5.2 RCCMD Installation mit vCenter 6 (ab RCCMD V 4.3.0.2) 138
4.2.6 RCCMD WebInterface Konfiguration auf ESXi 6.x (ab RCCMD V 4.3.0.2) 140
4.2.6.1 RCCMD WebInterface mit vCenter 6 (ab RCCMD V 4.3.0.2) 147
4.2.7 Alternative RCCMD Konfiguration über Editor 152
5. RCCMD auf Citrix XEN Server 154
6. RCCMD auf MAC OS 10.X 156
6.1 RCCMD WebInterface (ab Version 4.2.0.0) 161
6.2 RCCMD WebInterface Remote Zugriff 170
6.3 Alte RCCMD Konfiguration auf MAC OSX 170
7. RCCMD auf NovellNetWare 176
8. RCCMD auf DEC VMS 179
9. RCCMD AS400-Client 182
10. RCCMD FAQ 182
Appendix 187
A OpenSSL 187
B Syntax zum Schalten von Ausgängen 187
C Know How Pool 188
D RARITAN Dominion PDU Konfiguration 188
E Abbildungen 191

1. Was ist die RCCMD Software?

RCCMD ist eine Netzwerk Client Software, die das Empfangen von Shutdowns und Nachrichten von USV Servern wie UPSMAN UPS Software, CS121 SNMP Adapter oder jeder anderen RCCMD kompatiblen Netzwerkkarte von anderen, lizensierten Partnern ermöglicht.

RCCMD ist die erfolgreichste *Multiple Server Shutdown Software* und *Nachrichten Tool* in der gesamten USV Welt.

1.1 Netzwerk Shutdown mit RCCMD

Das Programm RCCMD wurde entwickelt, um Befehle auf einem Remote System in einem TCP/IP Netzwerk auszuführen. RCCMD arbeitet wie das RSH (Remote Shell), das man aus der UNIX Umgebung kennt. Innerhalb der UPS Management Software wird RCCMD zum Herunterfahren von mehren Servern benutzt, die alle von einer einzelnen USV versorgt werden. Für diese Aktion wurde einer dieser Server als *UPS Master Server* konfiguriert.

Installieren Sie die UPS Management Software *UPSMAN* auf ihrem UPS Master Server und verbinden Sie ihn mit der USV. Alternativ können Sie einen CS121 SNMP Adapter verwenden. Die anderen Server sind nur mit der USV Stromversorgung verbunden, da keine RS232 Verbindung notwendig ist. Installieren Sie RCCMD auf diesen Remote Maschinen, und erstellen Sie eine Shutdown-Routine für jedes System. Diese Shutdown-Routine könnte ein Batch File, ein Shell Script oder NFC File sein, das die Befehle für dieses Sytem beinhaltet. Danach fügen Sie RCCMD zu der Shutdown-Aktion oder der Event Konfiguration des UPS Master Servers hinzu.

Nun haben Sie eine Workstation in ihrem Server Netzwerk, die die USV überwacht. Die anderen Server führen RCCMD aus und erwarten das RCCMD Signal von dem USV Master Server. Im Falle eines Stromausfalls würde der Master ein Shutdown-Signal für das Server Netzwerk wie folgt veranlassen. Die Shutdown-Aktion des USV Master Servers würde RCCMD starten und ein entsprechendes Signal an alle Server in der Liste senden. RCCMD würde den programmierten Befehl auf den Empfängern ausführen.

Bitte beachten Sie, dass es erforderlich ist, RCCMD in 2 verschiedenen Funktionen zu installieren:

1. Als Sender auf dem USV Master Server

   (RCCMD –s) (send)

2. Als Empfänger (Hintergrund Prozess) auf den Empfangs-Servern

   (RCCMD –l) (listen)

Im Gegensatz zu RSH, enthält RCCMD nicht den auszuführenden Befehl, der versendet wird, aber dafür setzt es den Befehl im Empfangs-Prozess ab. Dies bietet einen entscheidenden Sicherheitsvorteil im Gegensatz zu RSH. Darüber hinaus überprüft der Empfänger dabei, welche Workstation das RCCMD Signal sendet und entscheidet, ob der auszuführende Befehl akzeptiert wird oder nicht.

Achtung: **Wir empfehlen immer mit der IP Adresse einen Netzwerk Shutdown via RCCMD durchzuführen und nicht den Hostnamen zu verwenden.**

RCCMD Version 2 oder höher

Die erweiterte Version von RCCMD ist in der Lage, Befehle auf Remote Systemen, ein Shutdown Batch File in dem TCP/IP Port 6003, ein Email-Batch, Log File Einträge usw. auszuführen. Der RCCMD 2 Sender (UPSMAN oder CS121 SNMP Adapter) sendet ein entsprechendes RCCMD Signal, und der RCCMD 2 Client startet das entsprechende Batch File.

Der initiierte Befehl wird immer vom UPSMAN oder dem CS121 gesendet, welcher auf dem RCCMD Client ausgeführt wird.

Beispiel: Der CS121 soll eine NET SEND (Netzwerknachricht) in ein Windows NT Netzwerk senden. Der Adapter kann so konfiguriert werden, dass er während eines Stromausfalls eine RCCMD Message gesendet wird, die individuell vom Benutzer verfasst werden kann.

Beim Empfangen der Nachricht startet der RCCMD 2 Client ein Batch File und sendet die NET SEND Message. Initiator ist hierbei der UPSMAN oder der CS121. Dadurch ist es möglich, Nachrichten oder Emails in unterschiedliche Netzwerke mit verschiedenen Betriebssystemen zu senden, initiiert durch einen USV Alarm.

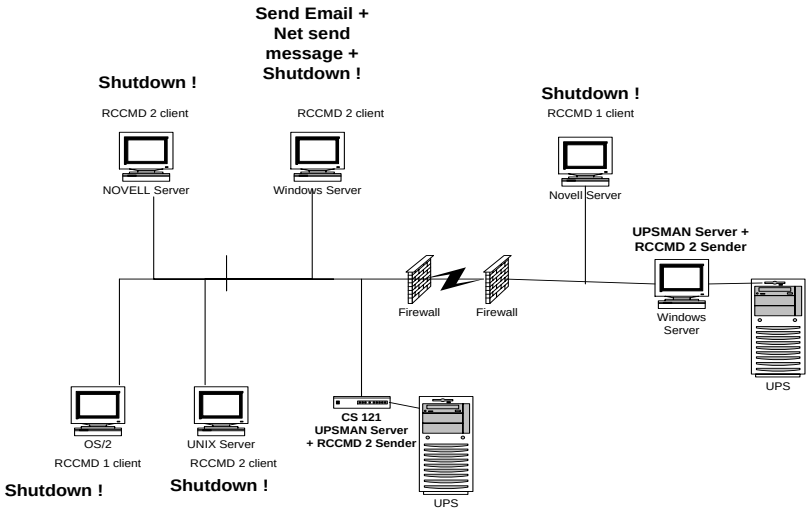

Abb. 1: RCCMD und UPSMAN in einer Netzwerkumgebung

2. Installation / Konfiguration von RCCMD für Windows

Hinweis:

Der RCCMD Installer verwendet die von uns mitgelieferte Java Runtime Version, die nur für die Installation bzw. Deinstallation verwendet wird. Zusätzlich verwendet der RCCMD Web Configurator einen Java Webserver (jetty). Den RCCMD Dienst RCCMDWebIf kann man in der Verwaltung deaktivieren, dann verwendet RCCMD kein Java mehr!

2.1 Installation von RCCMD

Bevor Sie mit der Installation beginnen, sollten Sie sich vergewissern, dass Sie über volle Administrator Rechte verfügen.

Step 1:	Legen Sie die CD in das Laufwerk ihres Computers, oder laden Sie die Software in ein Verzeichnis ihrer Wahl herunter.
Step 2:	Führen Sie die “installRCCMD.exe” aus, kopieren Sie die Daten auf ihre Festplatte, und wählen Sie die gewünschte Sprache aus.
Step 3:	Tragen Sie den Lizenzschlüssel in das Feld ein und wählen Sie das entsprechende Betriebssystem aus. Die Lizenz ermittelt, für welches Modul die Installation geeignet ist.

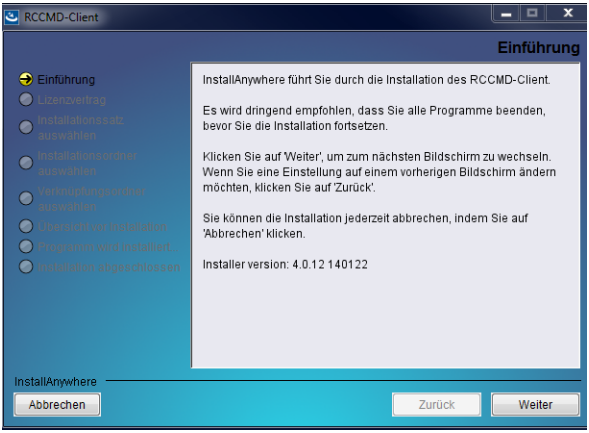
RCCMD-Client
Einführung
Einführung
Lizenzvertrag
Installationssatz auswählen
Installationsordner auswählen
Verknüpfungsordner auswählen
Übersicht vor Installation
Programm wird installiert...
Installation abgeschlossen
InstallAnywhere führt Sie durch die Installation des RCCMD-Client.
Es wird dringend empfohlen, dass Sie alle Programme beenden, bevor Sie die Installation fortsetzen.
Klicken Sie auf 'Weiter', um zum nächsten Bildschirm zu wechseln. Wenn Sie eine Einstellung auf einem vorherigen Bildschirm ändern möchten, klicken Sie auf 'Zurück'.
Sie können die Installation jederzeit abbrechen, indem Sie auf 'Abbrechen' klicken.
Installer version: 4.0.12 140122
InstallAnywhere
Abbrechen
Zurück
Weiter

Abb. 2: Einführung

In dem Menü auf der linken Seite des Fensters, können Sie den Fortschritt der Installation erkennen. Klicken Sie auf “Weiter”, um fortzufahren.

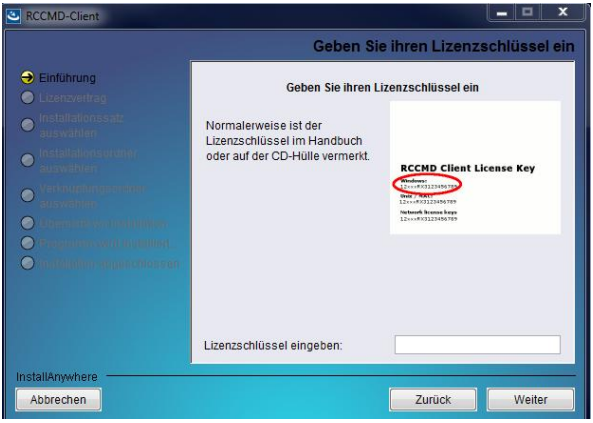

Abb. 3: Lizenzschlüssel Eintrag

Geben Sie hier Ihre Lizenznummer ein, ein Bild mit rotem Rahmen zeigt ein Beispiel. Klicken Sie auf “Next”, um fortzufahren.

Achtung:

Wird an dieser Stelle eine falsche Lizenznummer eingegeben, ist die RCCMD ClientSoftware auf eine 30 Tage Trial-Version eingestellt. Bitte informieren Sie sich bei Ihrem USV Händler nach der vollständigen Lizenz, falls diese nicht der Original CD beilag.

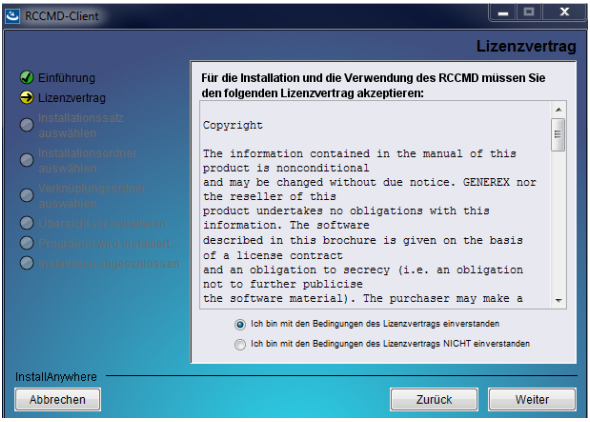
RCCMD-Client
Lizenzvertrag
Einführung
Lizenzvertrag
Installationssatz auswählen
Installationsordner auswählen
Verknüpfungsordner auswählen
Übersicht vor Installation
Programm wird installiert
Installation abgeschlossen
Für die Installation und die Verwendung des RCCMD müssen Sie den folgenden Lizenzvertrag akzeptieren:
Copyright
The information contained in the manual of this product is nonconditional and may be changed without due notice. GENEREX nor the reseller of this product undertakes no obligations with this information. The software described in this brochure is given on the basis of a license contract and an obligation to secrecy (i.e. an obligation not to further publicise the software material). The purchaser may make a
Ich bin mit den Bedingungen des Lizenzvertrags einverstanden
Ich bin mit den Bedingungen des Lizenzvertrags NICHT einverstanden
InstallAnywhere
Abbrechen
Zurück
Weiter

Abb. 4: Lizenzvertrag

Lesen und bestätigen Sie den Lizenzvertrag, und klicken sie auf “Weiter”.

Wählen Sie die Featues aus, die Sie installieren möchten.

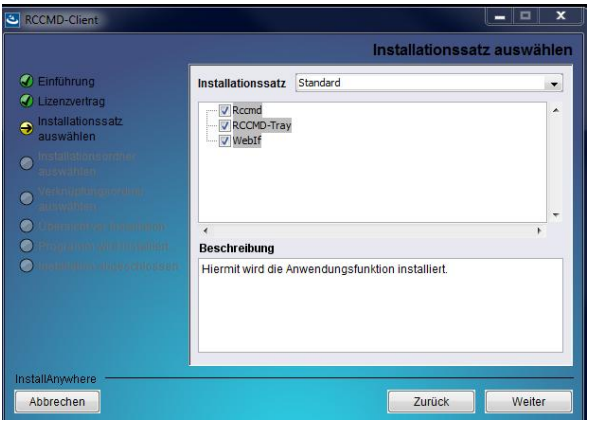

Abb. 5: Installationssatz Auswahl

Wählen Sie einen Zielordner aus.

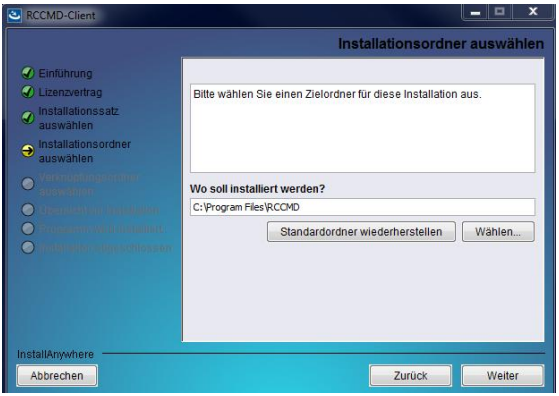

Abb. 6: Installationsordner Auswahl

Geben Sie den Pfad an, in dem Sie die Software installieren möchten. Standard ist das Verzeichnis C:\Program Files\RCCMD auf der Festplatte “C:\”.

Attention:

Wenn Sie ein Programm oder Batchfile mit RCCMD ausführen möchten, ist es erforderlich, dass dieses Programm oder Batchfile im Installationsverzeichnis C:\RCCMD (oder auch andere lokale Festplattenverzeichnisse, aber *nicht* in \Program Files\RCCMD wie bei einer Standardinstallation) liegt oder auf dem Verzeichnis ein Suchpfad gesetzt ist.

Im nächsten Fenster wird signalisiert, dass für die RCCMD.exe (6003, 5769 TCP/UDP), die RCCMDTray.exe (971 TCP) und RCCMD Weblf (8080 TCP) Firewall Ausnahmen erzeugt werden.

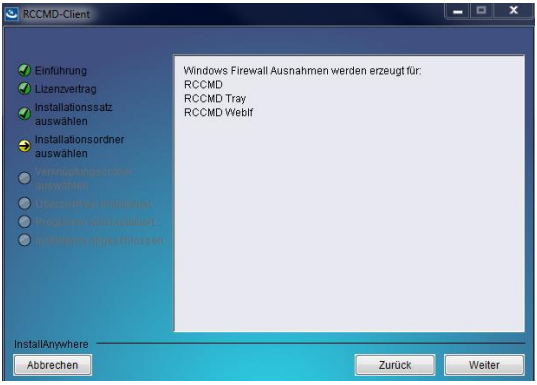

Abb. 7: Firewall Ausnahmen

Der RCCMD Tray ermöglicht das Erscheinen der RCCMD Nachrichten Box als Pop-Up im Vordergrund. Wenn Sie keine Nachrichten von RCCMD als Nachrichten Box erhalten wollen, dann schliessen Sie bitte den RCCMD Tray. Um den RCCMD Tray dauerhaft auszuschalten, können Sie in der RCCMD Konfiguration „Show Tray Icon“ ausschalten.

Der RCCMD Tray erscheint als Symbol in der Taskleiste.

Der rote Punkt bedeutet, dass der RCCMD Dienst nicht gestartet ist bzw. das ein Problem (USV-Kommunikation, Stromausfall) aufgetreten ist. Grün bedeutet, dass der Status okay ist.

Abb. 8: RCCMD Tray

In dem nächsten Menü können Sie eine neue Programmgruppe erstellen, deren Bestimmungsort festlegen oder eine Verknüpfung auf dem Desktop erstellen.

Abb. 9: Auswahl Verknüpfungsordner

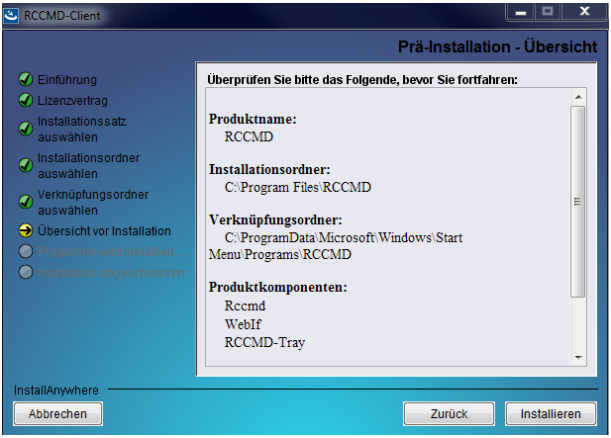

Abb. 10: Prä-Installations Übersicht

Klicken Sie auf “Installieren”, um fortzufahren.

Während der Installation wird überprüft, ob der Standard Port 8443 TCP des RCCMD WebConfigurators frei ist. Ausserdem haben Sie die Möglichkeit, vor Abschluss der Installation das Zugriffsprotokoll und den RCCMD WebIf Port zu ändern.

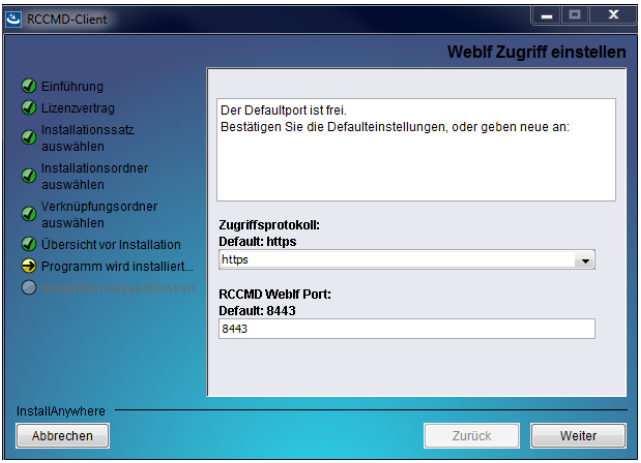

Abb. 11: Weblf Zugriff einstellen

Abb. 12: Kennworteingabe

Abb. 13: Passworthinweis-Eingabe

Somit ist die RCCMD Software erfolgreich installiert!

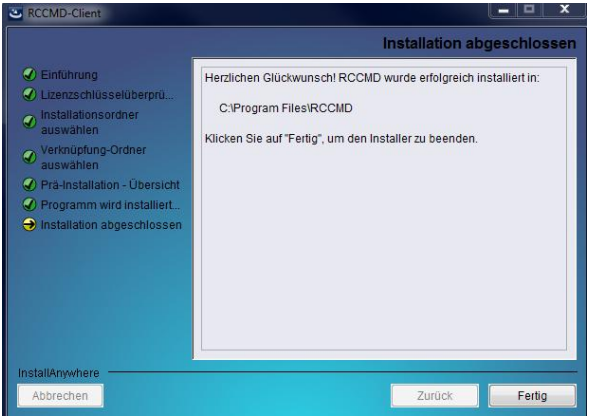

Abb. 14: Installations Abschluss

2.1.1 Silent Installation für die RCCMD Installation

In der RCCMD Software besteht die Möglichkeit, eine Silent Installation (Hintergrundinstallation) zu aktivieren. Bevor man diese Funktion nutzen möchte, sind Einstellungen in der Datei „installer.properties“ notwendig. Diese befindet sich auf der UPS Management CD im Verzeichnis \Rccmd\Windows\12:

Usage:

#

To record a new response file start the installer from command line

with parameter '-r'.

Use the new Values for the provided Variables from this file.

#

To perform a silent install, start the installer on the commandline.

The installer also needs the parameters '-f <path/to/resonsefile>'.

Choose Install Folder

Uncomment this variable to set a new default Folder into which the program will be installed.

The example represents the default, that will be used, if no folder is provided.

According to the example backslash characters ('\') need to be escaped by a backslash.

Spaces in the path also require a backslash as an escape character.

USER_INSTALL_DIR=C:\\RCCMD

Choose Link Location

You can tell the installer in which folder the shortcuts should be installed.

The absolute path must be given.

options are: "Do Not Install" if you do not want any shortcuts,

or a path to the folder in which the shortcuts should be created.

Here are two examples:

USER_SHORTCUTS=Do Not Install

USER_SHORTCUTS=C:\\Dokumente und Einstellungen\\<Windows User>\\Startmenü\\Programme\\UPS

Choose Feature List

If you want to install a subset of features from this installer,

make a list of all the features you want to be installed.

The List must be entered in the CHOSEN_INSTALL_FEATURE_LIST variable.

Options for the list are: RCCMD, WebIf

CHOSEN_INSTALL_FEATURE_LIST=RCCMD,WebIf

Choose OEM

Enter your OEM number here.

OEM=0

Choose locatization

If you want to install a different language than English

you will want to provide the valid country code here

This is only important for silent installations.

Valid codes are: zh_cn, de, en, fr, el, it, ja, ko, pt, ru, es, tr

INST_LANG=de

Choose License Key

For silent installation your License Key must

be provided here.

GXLICENSEKEY=yournumber

Choose Installer User Interface

For installation in console modus, pass the parameter: "-i console" to

the installer.

If you want to use the installer in silent mode with no user interaction,

you can set this variable to "silent".

Default is "gui".

INSTALLER_UI=silent

#INSTALLER_UI=gui

WebIf Settings

Here you can override default settings for access to the RCCMD WebIf.

These settings are ignored, if the variable CHOSEN_INSTALL_FEATURE_LIST

is set and does not contain the WebIf feature.

In interactive install modes (gui, console) the installer will check, whether

the chosen port is free to be used.

Valid values are: 1-65535

WEBIF_PORT=8080

Valid protocols are: http, https

WEBIF_PROTOCOL=http

Abb. 13: Dateiinhalt „installer.properties“

Um die Silent Installation zu aktivieren, müssen Sie das Doppelkreuz vor der Variablen `INSTALLER_UI=silent` entfernen. Zusätzlich ist die Eingabe eines Lizenzschlüssels hinter der Variablen `GXLICENSEKEY=` erforderlich. Wenn Sie die RCCMD Software nicht in das Standardverzeichnis `C:\Program Files\RCCMD` installieren möchten, beachten Sie bei der Eingabe des Installationspfades, dass das Backslash-Zeichen ein Backslash-Zeichen und ein Leerzeichen im Pfad ebenfalls ein Backslash-Zeichen benötigen, z. B.:

```
USER_INSTALL_DIR=C:\\program\ files\\RCCMD
```

Die Sprachauswahl können Sie mit der Variabel INST_LANG=de treffen, damit Ihnen bei der Konfiguration von der RCCMD Software die Tooltipps in der gewünschten Sprache zur Verfügung stehen.

2.1.2 RCCMD Silent Installation mit Übernahme eigener Konfiguration

Nach dem Sie die Datei „installer.properties“ ensprechend bearbeitet haben, ist es möglich, eine eigene RCCMD Konfiguration zu erstellen und „silent“ zu installieren. Dazu ist es erforderlich, die RCCMD Konfiguration einmal manuell durchzuführen via normal SETUP über den RCCMD Wizard.

Danach kann diese Konfiguration aus der Registry wie folgt in eine Datei exportiert werden:

- Klicken Sie mit der rechten Maustaste in dem Verzeichnis HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\rccmd\ auf „Parameters“, wählen „Export“ aus, und speichern Sie die Datei als „WIN95/NT4 Registration File mit dem Namen „rccmd.reg“.

- Legen Sie die Datei „rccmd.reg“ in das Verzeichnis ab, in dem sich das RCCMD-Installer-Paket befindet.

- Öffnen Sie die Datei „rccmd.reg“ mit einem Editor, und löschen Sie die komplette Zeile, die den Lizenzschlüssel enthält.

- Erstellen Sie mit einem Editor eine neue Windows-Batch-Datei (* .bat), zum Beispiel mit dem Namen „InstallAndConfigRCCMD.bat“, deren Inhalt wie folgt aussehen sollte:

```
@echo off
cls
echo *** Installation of RCCMD, please wait... ***
installRCCMD.exe
echo *** Importing RCCMD configuration file ***
regedit.exe -s rccmd.reg
echo Ready
```

Nun können Sie eine kombinierte RCCMD Silent Installation und Konfiguration starten, in dem Sie die soeben erstellte Windows-Batch-Datei „InstallAndConfigRCCMD.bat“ ausführen.

Klicken Sie auf “Installieren”, um fortzufahren.

2.2 Console Installation für die RCCMD Installation

Diese Konsolen-Installation arbeitet interaktiv und wird die im „installer.properties“ aufgeführten Fragen auf der Konsole ausgeben, die der Benutzer beantworten muss.

Hinweis: Dies betrifft nur die Installation, die Konfiguration wird mittels Editor in der Datei „rccmd.cfg“ ausgeführt.

Um die Console Installation zu aktivieren, müssen Sie das Doppelkreuz vor der Variabel `INSTALLER_UI=` entfernen und `console` eintragen. Dies ist die interaktive RCCMD Installation auf der Konsole. Führen Sie die **„installRCCMD.exe“** via Doppelklick aus.

Die Sprachauswahl können Sie mit der Variabel INST_LANG=de treffen, damit Ihnen bei der Konfiguration von der RCCMD Software die Tooltipps in der gewünschten Sprache zur Verfügung stehen.

2.2.1 Beispiel einer Console Installation

Ändern Sie die Datei „installer.properties“ entsprechend wie oben beschrieben ab, oder führen Sie einfach den Befehl **installRCCMD.exe –i console** aus.

Wählen Sie die gewünschte Sprache aus, und beachten Sie die Einführung.

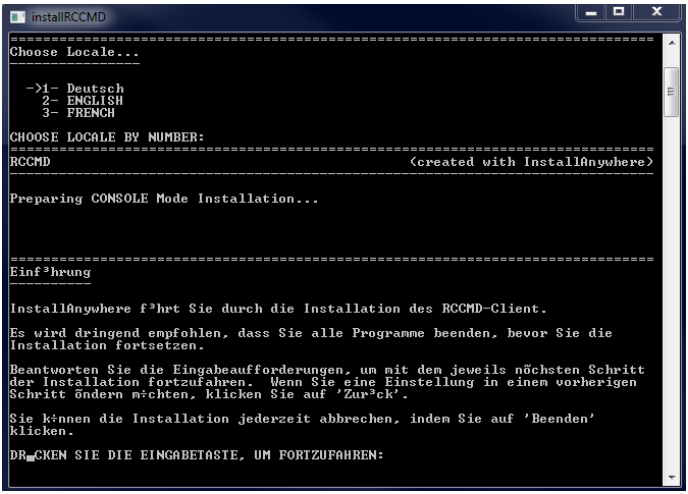
installRCCMD
Choose Locale...
->1- Deutsch
2- ENGLISH
3- FRENCH
CHOOSE LOCALE BY NUMBER:
RCCMD
(created with InstallAnywhere)
Preparing CONSOLE Mode Installation...
Einf³hrung
InstallAnywhere f³hrt Sie durch die Installation des RCCMD-Client.
Es wird dringend empfohlen, dass Sie alle Programme beenden, bevor Sie die Installation fortsetzen.
Beantworten Sie die Eingabeaufforderungen, um mit dem jeweils nächsten Schritt der Installation fortzufahren. Wenn Sie eine Einstellung in einem vorherigen Schritt ändern möchten, klicken Sie auf 'Zur³ck'.
Sie können die Installation jederzeit abbrechen, indem Sie auf 'Beenden' klicken.
DR_CKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 15: RCCMD Console Installation – Sprachauswahl, Einführung

Es folgt die Lizenzschlüssel Eingabe und der Lizenzvertrag.

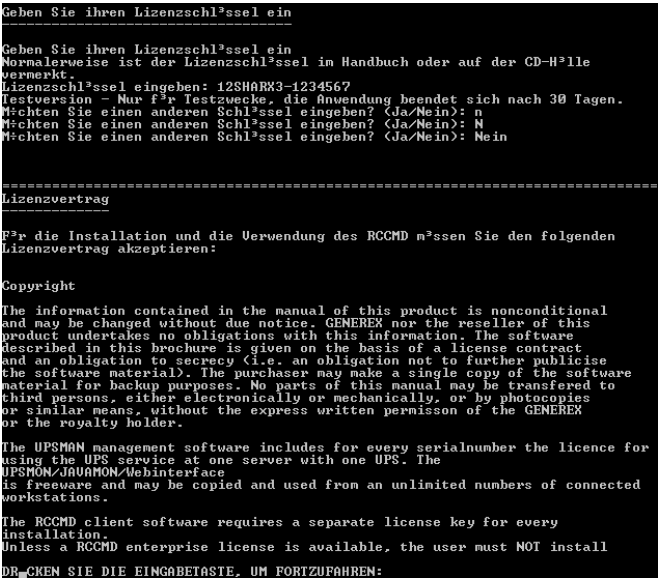
Geben Sie ihren Lizenzschl³ssel ein
Geben Sie ihren Lizenzschl³ssel ein
Normalerweise ist der Lizenzschl³ssel im Handbuch oder auf der CD-H³lle vermerkt.
Lizenzschl³ssel eingeben: 128HARX3-1234567
Testversion - Nur f³r Testzwecke, die Anwendung beendet sich nach 30 Tagen.
Möchten Sie einen anderen Schl³ssel eingeben? (Ja/Nein): n
Möchten Sie einen anderen Schl³ssel eingeben? (Ja/Nein): N
Möchten Sie einen anderen Schl³ssel eingeben? (Ja/Nein): Nein
Lizenzvertrag
F³r die Installation und die Verwendung des RCCMD m³ssen Sie den folgenden Lizenzvertrag akzeptieren:
Copyright
The information contained in the manual of this product is nonconditional and may be changed without due notice. GENEREX nor the reseller of this product undertakes no obligations with this information. The software described in this brochure is given on the basis of a license contract and an obligation to secrecy (i.e. an obligation not to further publicise the software material). The purchaser may make a single copy of the software material for backup purposes. No parts of this manual may be transfered to third persons, either electronically or mechanically, or by photocopies or similar means, without the express written permisson of the GENEREX or the royalty holder.
The UPSMAN management software includes for every serialnumber the licence for using the UPS service at one server with one UPS. The UPSMON/JAVAMON/Webinterface is freeware and may be copied and used from an unlimited numbers of connected workstations.
The RCCMD client software requires a separate license key for every installation.
Unless a RCCMD enterprise license is available, the user must NOT install
DR_CKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 16: RCCMD Console Installation – Eingabe Lizenzschlüssel, Lizenzvertrag

Wählen Sie die Produkt Features aus, die Sie installieren möchten, geben Sie einen Installations Pfad ein und beachten Sie die Firewall Ausnahmen.

Produktfunktionen auswählen
GEBEN SIE EINE DURCH KOMMAS GETRENNTE LISTE VON NUMMERN EIN, DIE FÜR DIE FUNKTIONEN STEHEN, DIE SIE AUSWÄHLEN BZW. DEREN AUSWAHL SIE AUFHEBEN MÖCHTEN. UM DIE BESCHREIBUNG EINER FUNKTION ANZUZEIGEN, GEBEN SIE '?<NUMMER>' EIN. UM DIE BESCHREIBUNG EINER FUNKTION ANZUZEIGEN, GEBEN SIE '?<NUMMER>' EIN. DRÜCKEN SIE DIE EINGABETASTE, WENN SIE FERTIG SIND.
1- [X] Rccmd
2- [X] WebIf
Wählen Sie die Funktionen aus, die vom Installer installiert werden sollen.
Installationsordner auswählen
Wo soll installiert werden?
Standardinstallationsordner: C:\Program Files\RCCMD
GEBEN SIE EINEN ABSOLUTEN PFAD EIN, ODER DRÜCKEN SIE DIE EINGABETASTE, UM DIE STANDARDEINSTELLUNG ZU ÜBERNEHMEN:
Firewall Ausnahmen
Windows Firewall Ausnahmen werden erzeugt für:
RCCMD
RCCMDTray
RCCMDWebIf
DRÜCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 17: RCCMD Console Installation – Produkt Auswahl, Pfad, Firewall Ausnahmen

Wählen Sie einen Pfad für die Links und beachten Sie die Installationsübersicht.

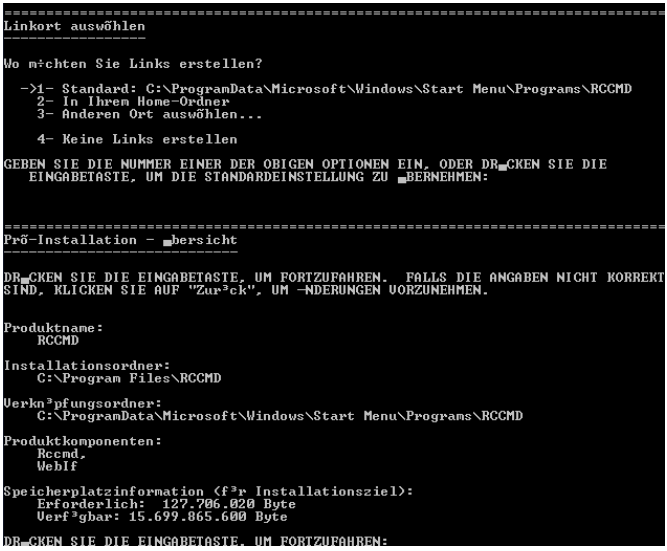
Linkort auswählen
Wo möchten Sie Links erstellen?
->1- Standard: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\RCCMD
2- In Ihrem Home-Ordner
3- Anderen Ort auswählen...
4- Keine Links erstellen
GEBEN SIE DIE NUMMER EINER DER OBIGEN OPTIONEN EIN, ODER DRÜCKEN SIE DIE EINGABETASTE, UM DIE STANDARDEINSTELLUNG ZU ÜBERNEHMEN:
Pre-Installation - Übersicht
DRÜCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN. FALLS DIE ANGABEN NICHT KORREKT SIND, KLICKEN SIE AUF "Zurück", UM ÄNDERUNGEN VORZUNEHMEN.
Produktname:
RCCMD
Installationsordner:
C:\Program Files\RCCMD
Verknüpfungsordner:
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\RCCMD
Produktkomponenten:
Rccmd,
WebIf
Speicherplatzinformation (für Installationsziel):
Erforderlich: 127.706.020 Byte
Verfügbar: 15.699.865.600 Byte
DRÜCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 18: RCCMD Console Installation – Link Pfad Auswahl, Installationsübersicht

Es folgt die Protokoll und Port Auswahl für das Web-Interface. Somit ist die Installation erfolgreich abgeschlossen.

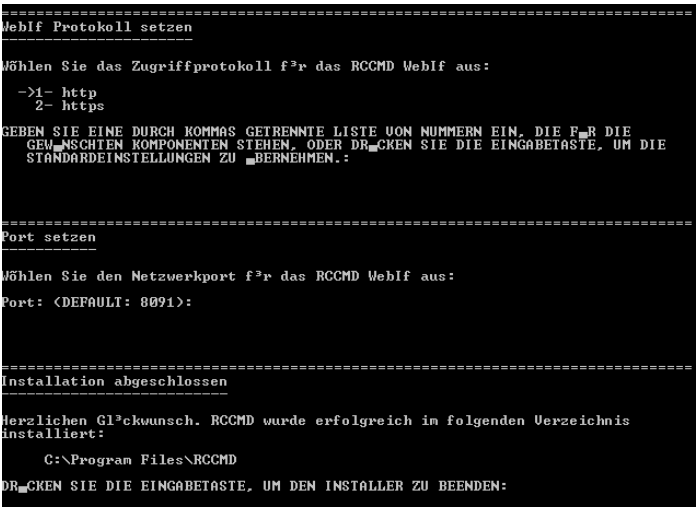
WebIf Protokoll setzen
Wöhlen Sie das Zugriffprotokoll f³r das RCCMD WebIf aus:
->1- http
2- https
GEBEN SIE EINE DURCH KOMMAS GETRENNTE LISTE VON NUMMERN EIN, DIE F▄R DIE GEW▄NSCHTEN KOMPONENTEN STEHEN, ODER DR▄CKEN SIE DIE EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ▄BERNEHMEN.:
Port setzen
Wöhlen Sie den Netzwerkport f³r das RCCMD WebIf aus:
Port: (DEFAULT: 8091):
Installation abgeschlossen
Herzlichen Gl³ckwunsch. RCCMD wurde erfolgreich im folgenden Verzeichnis installiert:
C:\Program Files\RCCMD
DR▄CKEN SIE DIE EINGABETASTE, UM DEN INSTALLER ZU BEENDEN:

Abb. 19: RCCMD Console Installation – WebIf Auswahl, Installations-Auswahl

2.2 RCCMD WebInterface (ab Version 4.0.1.9)

Ab der RCCMD Version 4.0.1.9 verfügt RCCMD über ein eigenes Webinterface, das die webbasierte Konfiguration bzw. Steuerung aus der Ferne ermöglicht. Nach der erfolgreichen Installation, wie in Kapitel 3.1 beschrieben, öffnet sich automatisch der Standardwebbrowser Ihres Betriebssystems.

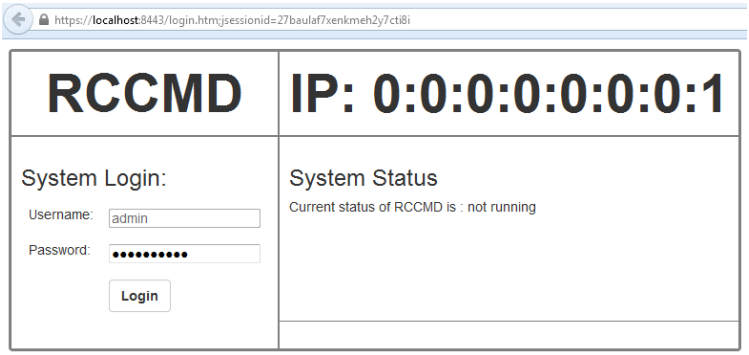

Abb. 20: RCCMD Configurator

Geben Sie das Passwort ein, das Sie während der installation angegeben haben.

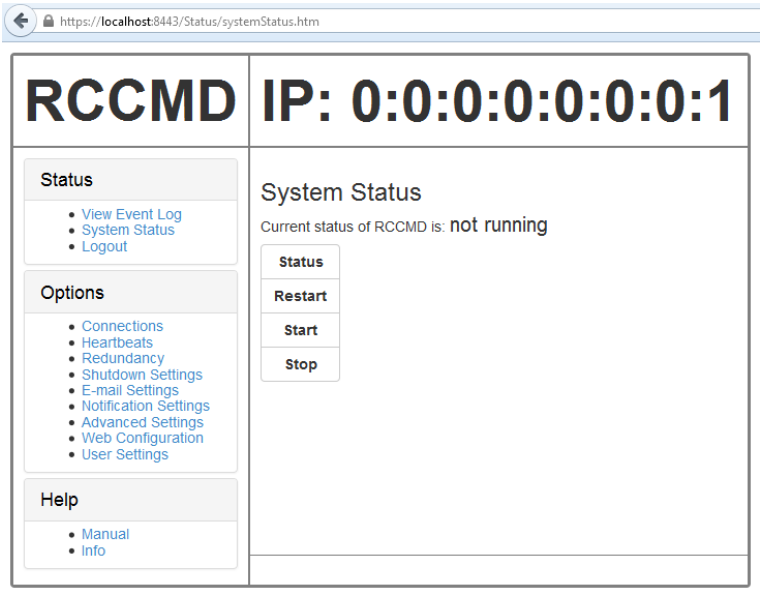

Abb. 21: RCCMD Configurator

Im Menü „**Connections**“ können Sie die IP-Adressen der berechtigten RCCMD Sender (CS121/UPSMAN) eintragen. Klicken Sie auf „Insert“, um die IP-Adresse des ersten Senders einzutragen. Klicken Sie auf „Remove“, wenn Sie die eingetragene IP-Adresse herausnehmen möchten. Klicken Sie auf „Edit“, wenn Sie die eingetragene IP-Adresse bearbeiten möchten.

Achtung: **Wenn Sie hier keine Adresse eintragen, ist jeder Server in der Lage, einen Shutdown an diesen Client zu senden.**

Unter „**Protocols**“ kann definiert werden, ob RCCMD mit SSL Zertifikaten verwendet wird. Aktivieren Sie „Reject expired SSL certificates“, wenn Sie Verbindungen mit abgelaufenen SSL Zertifikaten ablehnen wollen. Weitere Informationen für RCCMD mit SSL finden Sie in Kapitel 3.10.

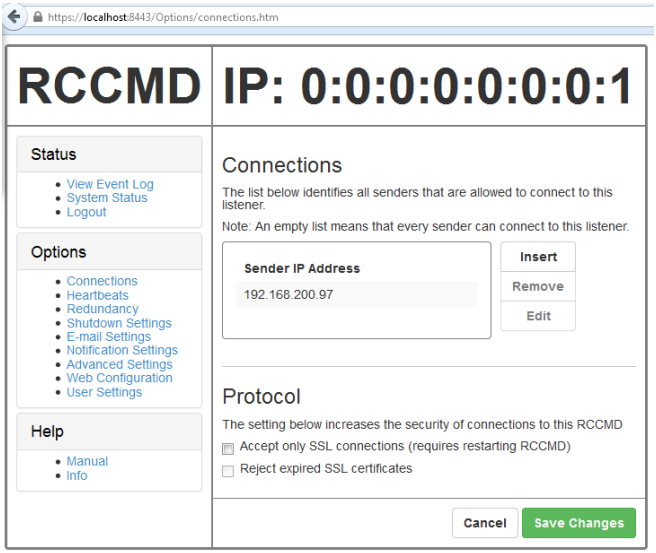

Abb. 22: RCCMD WebInterface Configurator – Connections

Klicken Sie vor Verlassen des „Connections“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Heartbeats**“ kann die Funktion „UPSMAN Alive Check“ aktiviert werden.

Dieser Check ist ein Signal, das an den CS121 oder UPSMAN via Port 5769 gesendet wird, um zu prüfen, ob der UPSMAN noch USV Daten hat. Wenn nicht, wird das Script File “Alive.Bat” ausgeführt, das eine entsprechende Nachricht als Pop-Up bringt.

Die Funktion “by the use CS121/UPSMAN Traps” ermöglicht UPSMAN/RCCMD/UNMS Meldungen, die den USV Status als Nachricht anzeigen. Wenn aktiviert, wird diese Funktion eine lokale Nachricht bringen, wenn der USV Status des UPSMAN/RCCMD Servers sich verändert.

Die Funktion „by polling CS121/UPSMAN every x seconds“ ermöglicht die reine Signalabfrage, ohne das Empfangen von USV-Werten bzw. Nachrichten.

Die Polling Rate (Standard 1800 Sekunden) definiert den Interval der UPSMAN Abfrage, connection retries (Verbindungswiederholungen, Standard 100) bedeutet, das nach 100 erfolglosen Verbindungsversuchen ein Alarm ausgelöst wird.

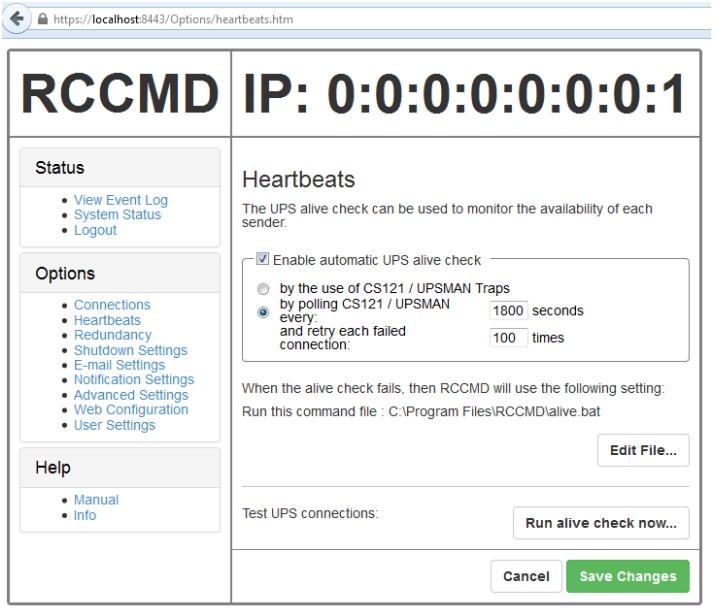

Abb. 23: RCCMD WebInterface Configurator – Heartbeats

Wenn Sie auf “Run alive check now…” klicken, wird das UPSMAN Alive Checking von der eingetragenen IP-Adresse gestartet (der Port 5769 wird getestet).

Klicken Sie vor Verlassen des „Heartbeats“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Redundancy**“ kann die Redundanz Management Funktion aktiviert werden. Der Redundanz Level definiert die Anzahl der redundanten Sender in der Redundanz Gruppe. Das bedeutet, dass bei einem Redunz Level von 1 beide RCCCMD Sender (CS121/UPSMAN) einen Shutdown gesendet haben müssen, bevor RCCMD seine Shutdown Sequenz startet.

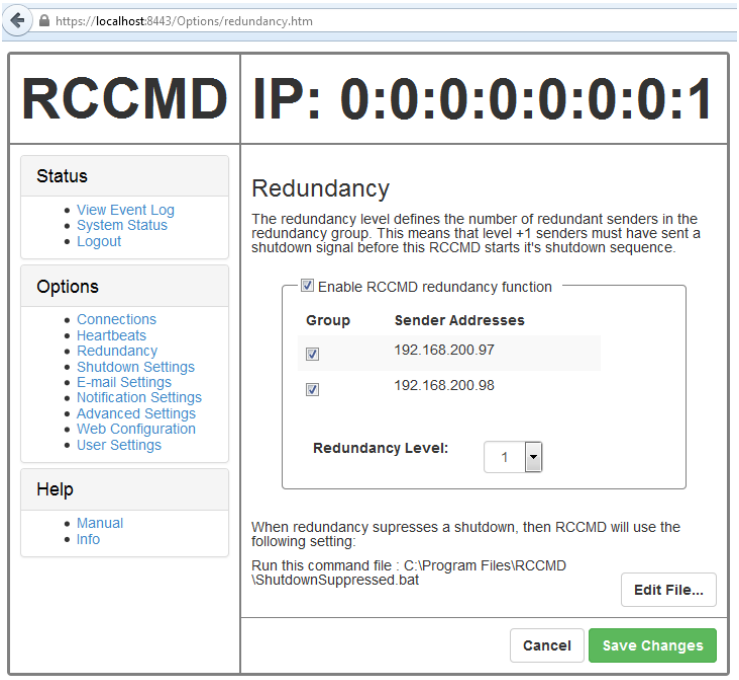

Abb. 24: RCCMD WebInterface Configurator – Redundancy

Wenn RCCMD einen Shutdown unterdrückt, erhalten Sie eine Nachrichten Box aus der „Suppressed.bat“, die Sie verändern können, wenn Sie auf „Edit File…“ klicken.

Bitte beachten Sie, dass für das Zurücksetzen des Redundanz Alarms eine Event Konfiguration auf dem Sender (CS121/UPSMAN) erforderlich ist. Die Funktion „Send RCCMD cancle shutdown“ kann verwendet werden, um automatisch einen vorher abgesendeten Shutdown zu verwerfen. Wenn ein Shutdown unterdrückt wurde, wegen der zu diesem Zeitpunkt noch vorhandenen Redundanz, das Problem aber zwischenzeitlich an der USV gelöst wurde, kann mittels einem „Send RCCMD cancel shutdown“ der Alarm zurückgesetzt werden. Durch diesen Befehl wird der RCCMD Client, der vorher das Shutdownsignal erhalten hat, aufgefordert, dieses wieder rückgängig zu machen.

Klicken Sie vor Verlassen des „Redundancy“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Shutdown Settings**“ können Sie die Shutdown Sequenz verändern bzw. erweitern. Als Standard wird die shutdown.bat verwendet:

rem created by setup

@echo off

set path=%path%;C:\Program Files\RCCMD

ExitWin.exe shutdown force

@cls

Die folgenden Befehle sind für die Shutdown Sequenz Konfiguration erhältlich:

Achtung: **Die Shutdown Sequenz wird von oben nach unten "abgearbeitet", d.h. der "Shutdown Windows" –Befehl sollte ganz unten in der Reihenfolge stehen, da danach natürlich keine weiteren Befehle mehr ausgeführt werden können.**

Shut down System: Beendet Ihre Sitzung und fährt Windows herunter, sodass Sie sicher die Stromzufuhr unterbrechen können.

Log Off from System: Beendet Ihre Sitzung, verlassen der Workstation, die im Betrieb bleibt.

Power off System: Beendet Ihre Sitzung, fährt Windows herunter und wird stromlos.

Restart System: Beendet Ihre Sitzung, fährt Windows herunter und startet es neu.

Hibernate System: Ist der Ruhestand, bei dem der Inhalt des Arbeitsspeichers auf die Festplatte geschrieben wird..

Suspend System: Ist der Ruhezustand, bei dem der Inhalt des Arbeitspeichers NICHT auf die Festplatte geschrieben wird.

Quit Lotus Notes: Schliesst Lotus Notes vor dem Herunterfahren von Windows. Bitte konfigurieren Sie eine Verzögerung nach diesem Befehl.

Quit Siemens SIMATIC: Schliesst die WIN CC Datenbank vor dem Herunterfahren von Windows. Bitte konfigurieren Sie eine Verzögerung nach diesem Befehl.

Quit Windows Applications: Schliesst alle Anwendungen vor dem Herunterfahren von Windows.

Wait some seconds: Wartet eine Weile in Sekunden, bis der nächste Befehl ausgeführt wird.

RCCMD shut down relay: Leitet einen RCCMD Shutdown Befehl an eine andere Workstation weiter.

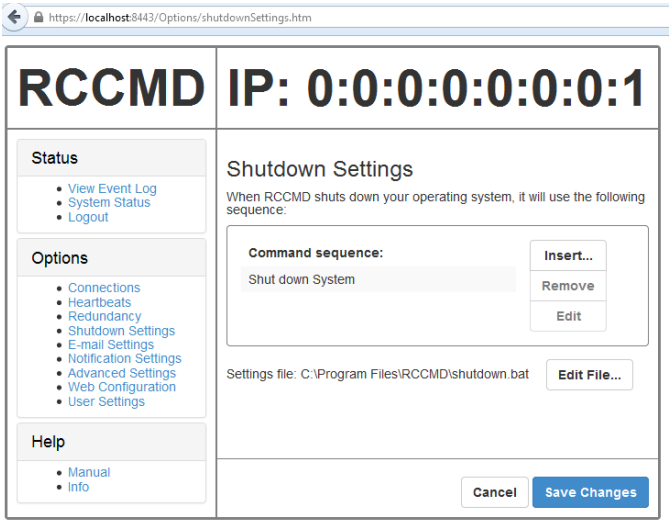

Abb. 25: RCCMD WebInterface Configurator – Shutdown Settings

Wenn Sie z. B. ein Powershell-Skript ausführen möchten, gibt es in den Shutdown Settings die Möglichkeit, Skripte einzufügen oder zu verändern. Wenn Sie die shutdown.bat verändern möchten, markieren Sie „Shut down System“, „Edit“ und danach auf „Save Changes“. Bitte beachten Sie, RCCMD neuzustarten.

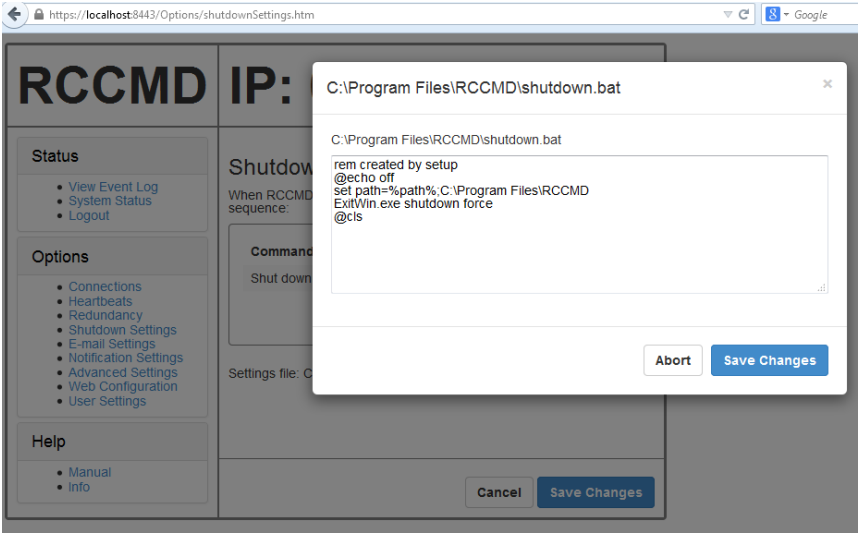

Abb. 26: RCCMD WebInterface Configurator – Shutdown Settings – Edit File

Im Menü **“E-mail Settings”** können die Email Einstellungen des Senders definiert werden. Zusätzlich kann hier die Verschlüsselung aktiviert werden und ggf. ein anderer SMTP Port angegeben werden.

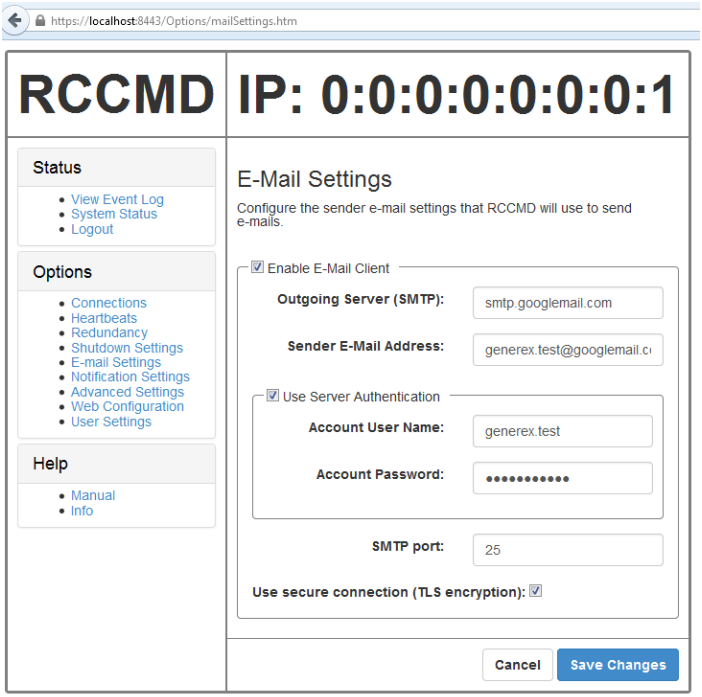

Abb. 27: RCCMD WebInterface Configurator – E-mail Settings

Im Menü „**Notification Settings**“ können Sie die entsprechenden Standard Bat-Files für E-Mail, Message (Nachrichten) und Execute (auszuführende Kommandos) verändern bzw. erweitern, wenn Sie auf „Edit File...“ klicken.

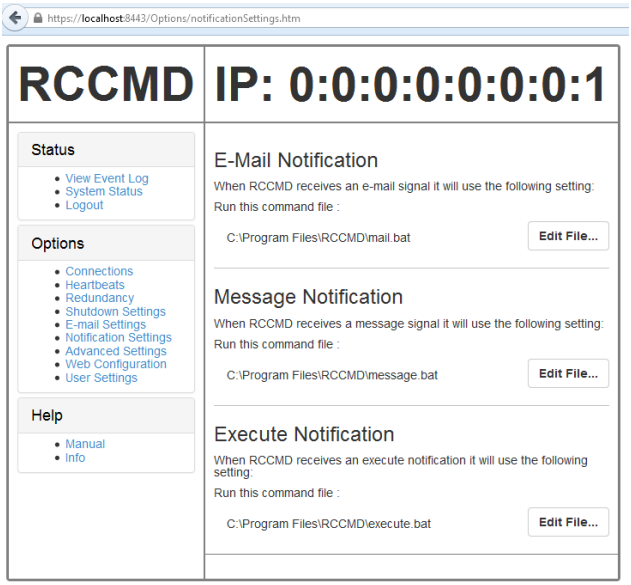

Abb. 28: RCCMD WebInterface Configurator – Notification Settings

Klicken Sie vor Verlassen des „Notification Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Advanced Settings**“ können Sie die maximale Grösse des Event Logfiles definieren, bei der das Überschreiben älterer Einträge beginnt, die RCCMD Bindings für die IP-Adresse und den RCCMD Listener TCP Port und den RCCMD Tray Message Port, über den die RCCMD Nachrichten gesendet werden.

Ausserdem besteht die Möglichkeit, die Funktion „Start Jobs as interactive User“ zu aktivieren“. Das bedeutet, dass RCCMD Jobs nur dann ausgeführt werden, wenn auf dem System irgendein Benutzer angemeldet ist und das RCCMD Tray aktiv ist.

Achtung: **Auch der Shutdown Job würde bei ausgeloggten Benutzer nicht ausgeführt werden! Bei Verwendung der Option „interactive user“ ist daher immer darauf zu achten, dass ein Benutzer eingeloggt ist!**

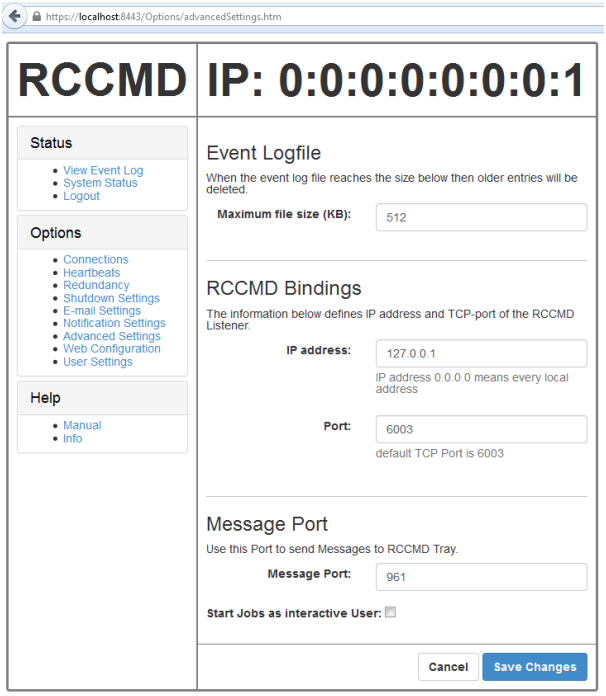

Abb. 29: RCCMD WebInterface Configurator – Advanced Settings

Klicken Sie vor Verlassen des „Advanced Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Web Configuration**“ besteht die Möglichkeit, das HTTPS Protokoll zu deaktivieren, um nur mit dem HTTP Protokoll zu arbeiten. Ab der RCCMD Version 4.0.2.1 gibt es zusätzlich die Möglichkeit, die Standard Ports für HTTP (8080) und HTTPS (8443) zu ändern.

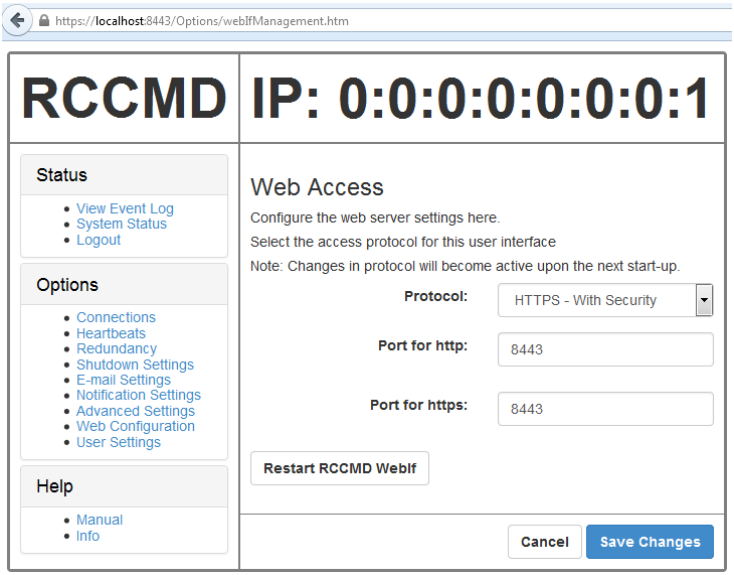

Abb. 30: RCCMD WebInterface Configurator – Web Configuration

Klicken Sie vor Verlassen des „Web Configuration“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern und danach den RCCMD WebIf Dienst neustarten.

Im Menü „**User Settings**“ können Sie das Standard Passwort für den Benutzer „admin“ wie gewünscht ändern und danach den RCCMD WebIf Dienst neustarten.

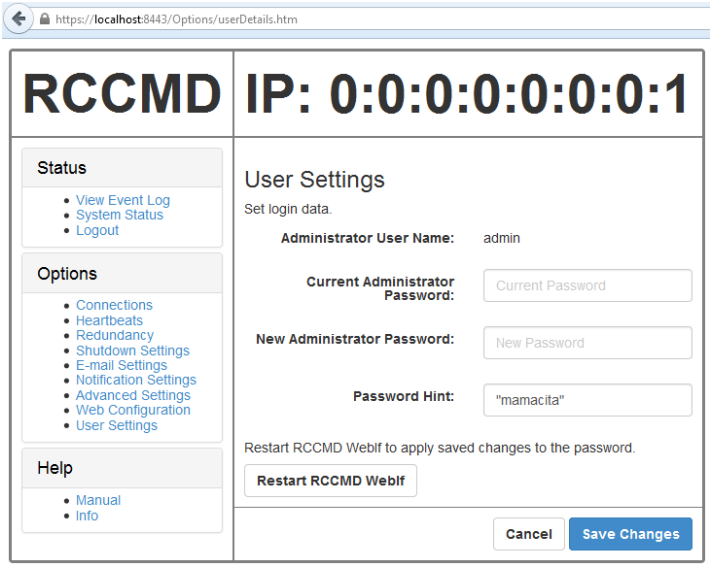

Abb. 31: RCCMD WebInterface Configurator – User Settings

Klicken Sie vor Verlassen des „User Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Klicken Sie auf „Logout“, wenn Sie den RCCMD Web Configurator nicht mehr benötigen.

Im Menü „**Status, View Event Log**“ können Sie die Protokollierung der bisherigen Ereignisse einsehen.

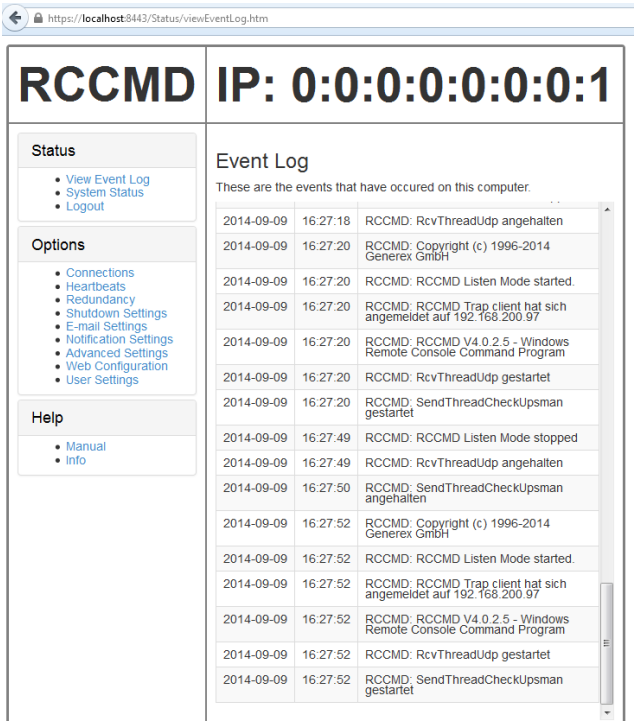
https://localhost:8443/Status/viewEventLog.htm
RCCMD
IP: 0:0:0:0:0:0:0:1
Status
View Event Log
System Status
Logout
Options
Connections
Heartbeats
Redundancy
Shutdown Settings
E-mail Settings
Notification Settings
Advanced Settings
Web Configuration
User Settings
Help
Manual
Info
Event Log
These are the events that have occured on this computer.
2014-09-09 16:27:18 RCCMD: RcvThreadUdp angehalten
2014-09-09 16:27:20 RCCMD: Copyright (c) 1996-2014 Generex GmbH
2014-09-09 16:27:20 RCCMD: RCCMD Listen Mode started.
2014-09-09 16:27:20 RCCMD: RCCMD Trap client hat sich angemeldet auf 192.168.200.97
2014-09-09 16:27:20 RCCMD: RCCMD V4.0.2.5 - Windows Remote Console Command Program
2014-09-09 16:27:20 RCCMD: RcvThreadUdp gestartet
2014-09-09 16:27:20 RCCMD: SendThreadCheckUpsman gestartet
2014-09-09 16:27:49 RCCMD: RCCMD Listen Mode stopped
2014-09-09 16:27:49 RCCMD: RcvThreadUdp angehalten
2014-09-09 16:27:50 RCCMD: SendThreadCheckUpsman angehalten
2014-09-09 16:27:52 RCCMD: Copyright (c) 1996-2014 Generex GmbH
2014-09-09 16:27:52 RCCMD: RCCMD Listen Mode started.
2014-09-09 16:27:52 RCCMD: RCCMD Trap client hat sich angemeldet auf 192.168.200.97
2014-09-09 16:27:52 RCCMD: RCCMD V4.0.2.5 - Windows Remote Console Command Program
2014-09-09 16:27:52 RCCMD: RcvThreadUdp gestartet
2014-09-09 16:27:52 RCCMD: SendThreadCheckUpsman gestartet

Abb. 32: RCCMD WebInterface Configurator – View Event Log

Im Menü „**Status, System Status**“ können Sie den aktuellen Status von RCCMD überprüfen, den Status updaten und den RCCMD Dienst neustarten bzw. stoppen und starten.

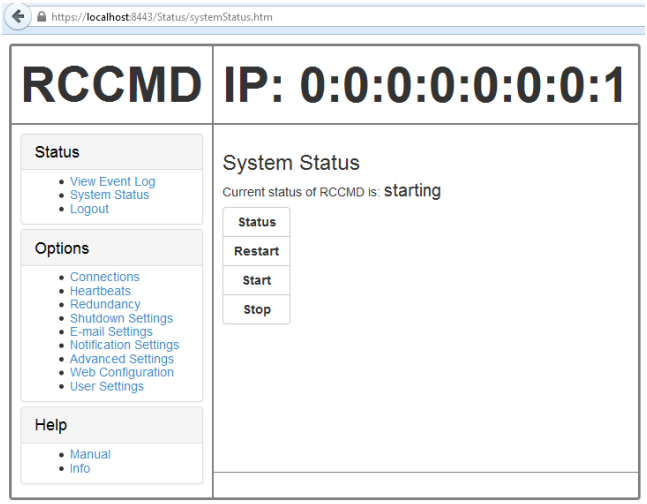

Abb. 33: RCCMD WebInterface Configurator – System Status

Im Menü „**Help**“ können Sie das RCCMD Benutzerhandbuch zu Ihrer Unterstützung aufrufen, können dem Link auf www.generex.de folgen und via „Info“ die Installer Version aufrufen.

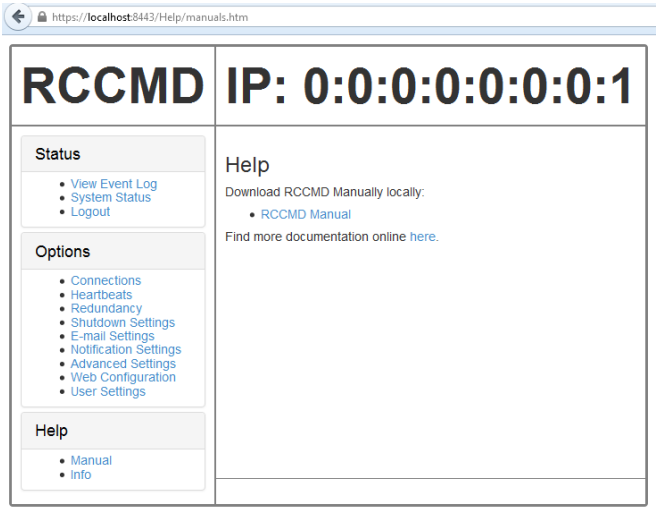

Abb. 34: RCCMD WebInterface Configurator – Help

2.2.1 RCCMD WebInterface Remote Zugriff

Ab der RCCMD Version 4.0.1.9 verfügt RCCMD über ein eigenes Webinterface, dass den Remote Zugriff ermöglicht. Bitte beachten Sie, dass der Firewall Port 8443 TCP

freigeschaltet sein muss. Geben Sie in einem Webbrowser Folgendes ein, um sich remote auf den Rechner zu verbinden, auf dem RCCMD installiert wurde

https://IP-Adresse des RCCMD Rechners:8443

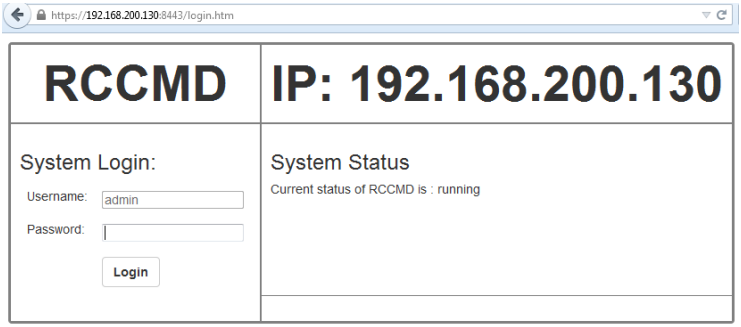

Abb. 35: RCCMD WebInterface Configurator – Remote Zugriff

Nun besteht die Möglichkeit, die Konfiguration bzw. Steuerung aus der Ferne auszuführen.

2.3 Der RCCMD Client als Relay Station

Wenn Sie eine grössere Anzahl von RCCMD Empfänger erreichen möchten, muss ein RCCMD Client als Relay Station fungieren. Der Empfänger wird so konfiguriert, dass er beim Erhalten eines RCCMD Signals eine Batch Datei startet, die weitere RCCMD Signale versendet. Diese Workstation ist dann Empfänger und Sender zur gleichen Zeit und somit eine wichtige Verbindung in der USV Überwachungskette. Der Gebrauch von einem RCCMD Client als Relay Station macht die Überwachung von mehreren hundert RCCMD Clients sehr viel einfacher als die Konfiguration über das Web-Interface des CS121. Außerdem haben alle Webbrowser Event Konfigurationen eine Sicherheits-limitierung, sodas es erforderlich ist, diese Relay Funktion zu nutzen, wenn die Anzahl der Jobs 50 pro Event auf dem CS121 HW131 übersteigt.

Sehen Sie in das folgende Script, das den RCCMD Client als Relay Station agieren lässt:

```
rem created by setup
@echo off
set path=%path%;C:\Program Files\RCCMD
# RELAY RCCMD
# This batch will send RCCMD shutdowns to the IP addresses listed below
# At the end of the batch this computer will initiate the local shutdown
start rccmd -s -a 192.168.200.2
start rccmd -s -a 192.168.200.3
start rccmd -s -a 192.168.200.4
start rccmd -s -a 192.168.200.5
start rccmd -s -a 192.168.200.6
start rccmd -s -a 192.168.200.7
# to be continued
#
# local shutdown
ExitWin.exe shutdown force
@cls
```

Abb. 36: Example: Batch File RCCMD als Relay Station

„start“ ist ein Windows Batchfile Kommando, um ein Programm-Aufruf in mehreren Instanzen zu starten. Dies ermöglicht das Ausführen von Programmen simultan und beschleunigt die Shutdown-Prozedur. Bitte beachten Sie, dass „start“ nicht auf allen Windows OS unterstützt wird und sollte getestet werden, bevor es verwendet wird.

2.4 Automatisches Zurücksetzen des Redundanz Alarms

„Send RCCMD cancle shutdown“ kann verwendet werden, um automatisch einen vorher abgesendeten Shutdown zu verwerfen. Wenn ein Shutdown unterdrückt wurde, wegen der zu diesem Zeitpunkt noch vorhandenen Redundanz, das Problem aber zwischenzeitlich an der USV gelöst wurde, kann mittels einem „Send RCCMD cancel shutdown“ der Alarm zurückgesetzt werden. Durch diesen Befehl wird der RCCMD Client, der vorher das Shutdownsignal erhalten hat, aufgefordert, dieses wieder rückgängig zu machen.

Dieses Kommando kann indivduell in jedem Event/Alarm ihrer CS121 oder BACS WEBMANAGER Konfiguration eingefügt werden, macht allerdings nur dann Sinn, wenn der Event, der diesen Befehl absendet, auch tatsächlich dann aktiv ist, wenn die USV wieder als OK angesehen werden kann. Dafür geeignet sind Beispielsweise die Events „POWER RESTORED“, “BATTERY LOW OFF”, “UPSMAN STARTED” und “GENERAL ALARM OFF”, wenn diese in ihrem CS121 für diesen USV Typ angeboten werden. In diese „Entwarnungs-Ereignnisse“ würde dann der Job „Send RCCMD cancle shutdown“ eingetragen werden, sodass z. B. beim Neustart der USV, der Event „UPSMAN STARTED“ automatisch den betreffenden RCCMD Client wieder auf „normal“ zurücksetzt.

Alternativ: Sollte der Job „Send RCCMD cancle shutdown“ in ihrem CS121, UPSMAN oder BACS WEBMANAGER nicht vorhanden sein, kann alternativ auch der Job „Send RCCMD Command to remote client“ oder „Send RCCMD execute to remote client“ verwendet werden.

Der Parameter „WAKEUP“ hat die gleiche Funktion wie „Send RCCMD cancle shutdown“ und setzt den Redundanz Level eines RCCMD Clients in den Ausgangszustand zurück.

Auch hier eignen sich die Events/Alarme POWER RESTORED, BATTERY LOW OFF, UPSMAN STARTED und GENERAL ALARM OFF besonders, um die Funktion „Send RCCMD Command to remote client“ mit dem „WAKEUP“ Befehl zu konfigurieren.

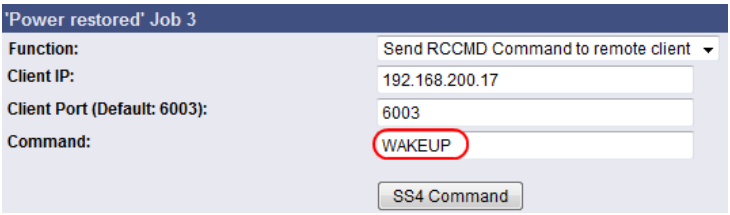

Abb. 37: CS121 Konfiguration „WAKEUP“ Befehl

Klicken Sie im CS121 Menü „Events/Alarms“ auf „Power restored“, und fügen Sie einen neuen Job hinzu. Wählen Sie die Funktion „Send RCCMD Command to remote client“ aus, tragen Sie die entsprechende IP-Adresse des Clients ein, und schreiben Sie den Befehl „WAKEUP“ in die „Command“ Zeile.

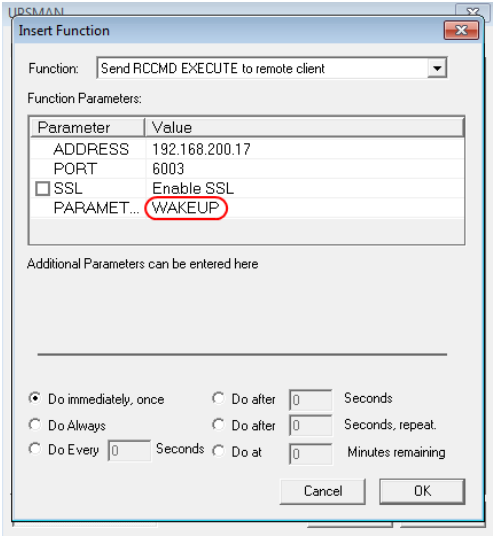

Abb. 38: UPSMAN Konfiguration „WAKEUP“ Befehl

Öffnen Sie die UPSMAN Konfiguration, und klicken Sie auf „Avanced Users“, „Events“, „Power restored“ und „Insert“. Fügen Sie die Funktion „Send RCCMD EXECUTE to remote client“ hinzu, und tragen Sie die entsprechende IP-Adresse des Clients ein, und schreiben Sie den Befehl „WAKEUP“ in die Parameter Zeile.

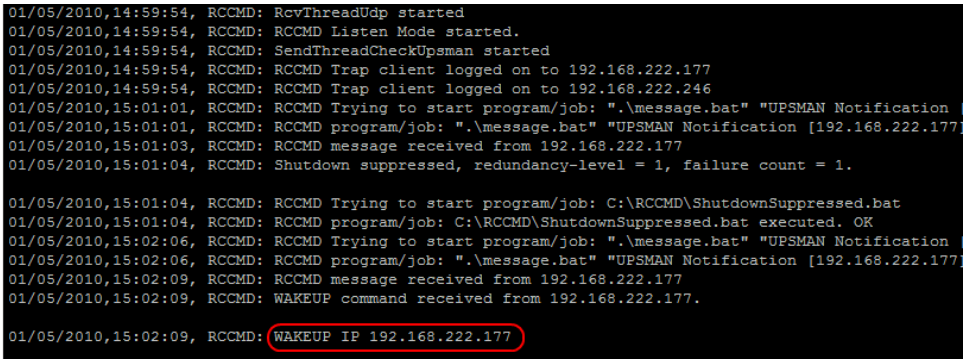
01/05/2010,14:59:54, RCCMD: RcvThreadUdp started
01/05/2010,14:59:54, RCCMD: RCCMD Listen Mode started.
01/05/2010,14:59:54, RCCMD: SendThreadCheckUpsman started
01/05/2010,14:59:54, RCCMD: RCCMD Trap client logged on to 192.168.222.177
01/05/2010,14:59:54, RCCMD: RCCMD Trap client logged on to 192.168.222.246
01/05/2010,15:01:01, RCCMD: RCCMD Trying to start program/job: ".\message.bat" "UPSMAN Notification
01/05/2010,15:01:01, RCCMD: RCCMD program/job: ".\message.bat" "UPSMAN Notification [192.168.222.177]
01/05/2010,15:01:03, RCCMD: RCCMD message received from 192.168.222.177
01/05/2010,15:01:04, RCCMD: Shutdown suppressed, redundancy-level = 1, failure count = 1.
01/05/2010,15:01:04, RCCMD: RCCMD Trying to start program/job: C:\RCCMD\ShutdownSuppressed.bat
01/05/2010,15:01:04, RCCMD: RCCMD program/job: C:\RCCMD\ShutdownSuppressed.bat executed. OK
01/05/2010,15:02:06, RCCMD: RCCMD Trying to start program/job: ".\message.bat" "UPSMAN Notification
01/05/2010,15:02:06, RCCMD: RCCMD program/job: ".\message.bat" "UPSMAN Notification [192.168.222.177]
01/05/2010,15:02:09, RCCMD: RCCMD message received from 192.168.222.177
01/05/2010,15:02:09, RCCMD: WAKEUP command received from 192.168.222.177.
01/05/2010,15:02:09, RCCMD: WAKEUP IP 192.168.222.177

Abb. 39: „WAKEUP“ Befehl im RCCMD Log

Hinweis: Das Neustarten des RCCMD Dienstes ist eine dritte Möglichkeit, um den Redundanz Alarm zurückzusetzen.

2.5 RCCMD mit SSL auf Windows

Das *Secure Sockets Layer* (SSL) Protokoll ist ein kryptografisches Protokoll, das Sicherheit und Datenintegrität für Kommunikationen in TCP/IP Netzwerken zusätzlich bietet. Bei einem Versand von RCCMD Nachrichten wird dann eine Verschlüsselung (auch mit eigenen Zertifikaten) verwendet und nur dann auf dem Client ausgeführt, wenn die Codes übereinstimmen und sich auch in einem gewissen Zeitrahmen (Zeitstempel) befinden.

Stellen Sie über einen Webbrowser eine Verbindung zum CS121 SNMP Adapter her. Klicken Sie im Konfigurations-Menü auf “Network & Security”, und setzen Sie den Haken bei “Use RCCMD SSL”.

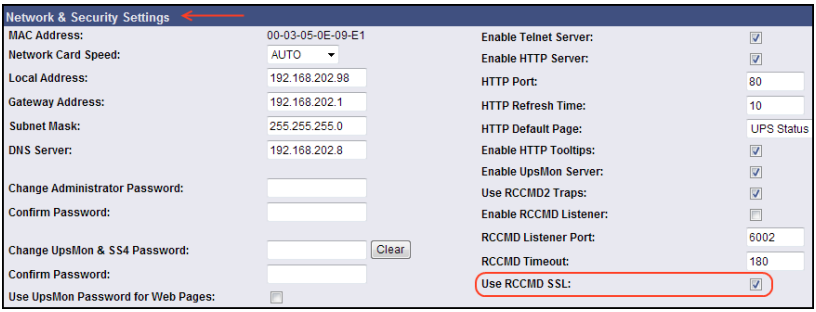

Abb. 40: RCCMD SSL Einstellung

Das SSL Netzwerk Feature erfordert einen korrekten Zeitstempel. Konfigurieren Sie im „Timeserver“ Menü eine entsprechende IP-Adresse.

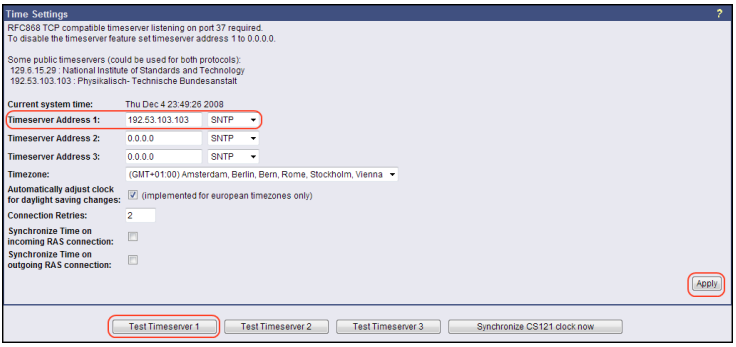

Abb. 41: Timeserver Konfiguration

Klicken Sie auf das „Save Configuration“ Menü, und bestätigen Sie Ihre Einstellungen mit „Save, Exit & Reboot“.

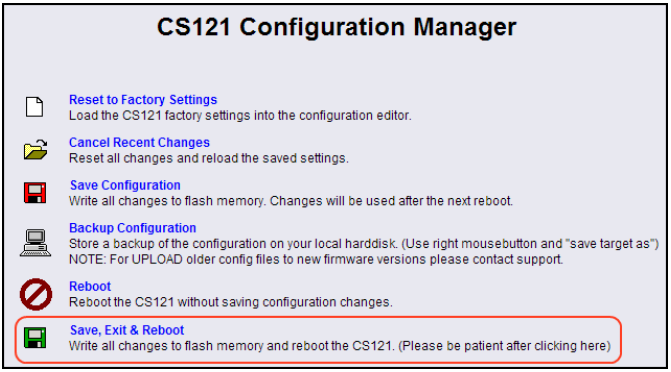
CS121 Configuration Manager
Reset to Factory Settings
Load the CS121 factory settings into the configuration editor.
Cancel Recent Changes
Reset all changes and reload the saved settings.
Save Configuration
Write all changes to flash memory. Changes will be used after the next reboot.
Backup Configuration
Store a backup of the configuration on your local harddisk. (Use right mousebutton and "save target as")
NOTE: For UPLOAD older config files to new firmware versions please contact support.
Reboot
Reboot the CS121 without saving configuration changes.
Save, Exit & Reboot
Write all changes to flash memory and reboot the CS121. (Please be patient after clicking here)

Abb. 42: Speichern der Einstellungen

Starten Sie den RCCMD Web Configurator erneut, und aktivieren Sie das SSL Feature.

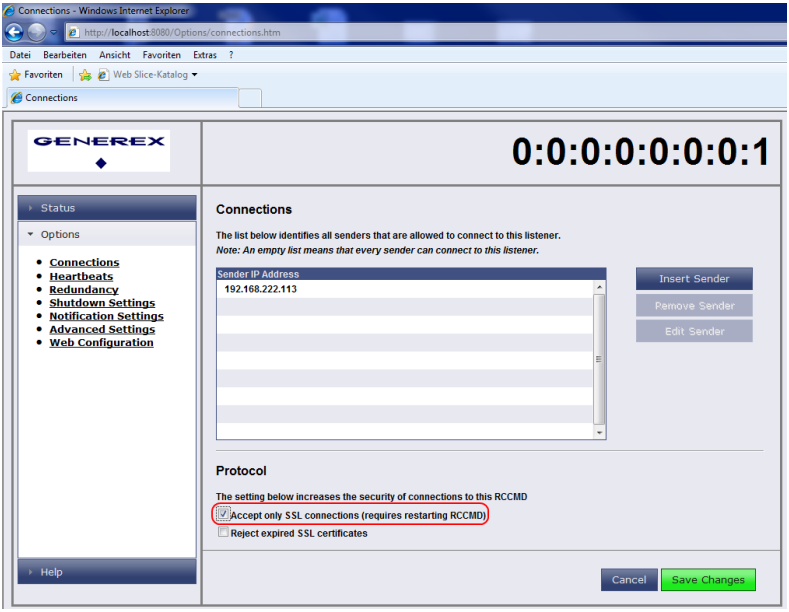

Abb. 43: SSL Konfiguration

Wenn Sie abgelaufene Zertifikate akzeptieren möchten, aktivieren Sie die Funktion “Reject expired SSL certificates”.

2.5.1 RCCMD mit eigenen SSL Zertifikaten

In diesem Abschnitt beschreiben wir, wie man ein eigenes SSL Zertifikat mit RCCMD nutzen kann, z. B. OpenSSL (http://www.openssl.org/related/binaries.html):

Erstellung eigener Zertifikate (CA)

Mit der Nutzung von OpenSSL ist es sehr einfach, sein eigener Zertifizierer zu werden. Nutzen Sie einfach diesen Befehl:

```
CA.pl -newca
```

Fertig! Vergewissern Sie sich, dass Sie einen gebräuchlichen CN (gewöhnlichen Namen) verwendet haben.

Erstellen des RCCMD Zertifikats

Nun müssen Sie Ihr Zertifikat für RCCMD erstellen. Da es für die Verifizierung den CN nutzt, sollte das Zertifikat diesen Namen auch enthalten, den Sie für das CA gewählt haben. Die private Schlüssel muss nicht verschlüsselt werden, um den RCCMD Client (Dienst) zu starten. Dafür nutzen wir die “-nodes” Option und den “-newreq” Befehl:

```
CA.pl -newreq -nodes
```

Signieren mit CA:

```
CA.pl -sign
```

Erstellen Sie nun eine leere Datei mit dem Namen “rccmd.pem”, und kopieren Sie die Zertifizierungsinformationen von “newcert.pem” (RCCMD Zertifikat), “newkey.pem” (Privater Schlüssel) und “cacert.pem” (CA) in diese Datei. Bitte beachten Sie, dass das exakte Kopieren erforderlich ist, damit Sie es ohne Probleme nutzen können.

Nutzung des eigenen RCCMD Zertifikats

Führen Sie die folgenden Schritte auf jedem RCCMD Client und Sender aus, um die Konfiguration abzuschliessen.

- Stellen Sie ein Backup von der existierenden “rccmd.pem” her
- Ersetzen Sie die “rccmd.pem” mit Ihrer eigenen
- Starten Sie den RCCMD Client neu

Starten Sie den RCCMD Sender neu!

2.6 Einstellungen der Berechtigung für den RCCMD Dienst

Diese Funktion wird benötigt, um Benutzerrechte dem UPSMAN Dienst zu übergeben, die über den System-Shutdown hinausgehen, z. B. starten eines Skriptes, Batchfiles etc..

Öffnen Sie das Eigenschaften-Menü für den RCCMD Dienst (via Systemsteuerung, Verwaltung, Dienste).

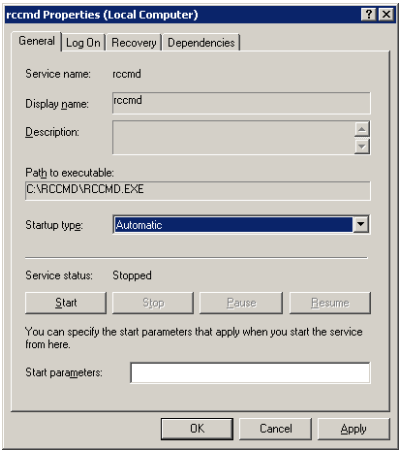

Abb. 44: RCCMD Eigenschaften Fenster

Klicken Sie auf den Kartenreiter “Log On”.

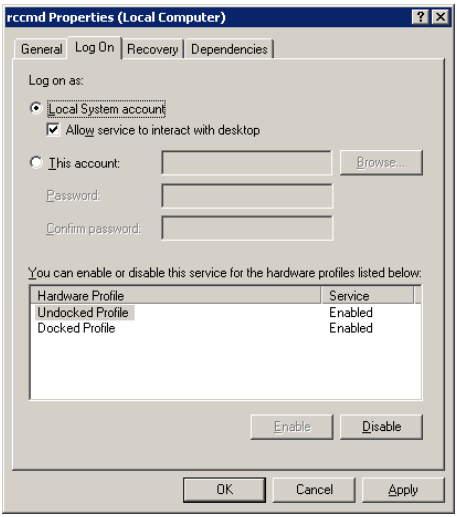

Abb. 45: RCCMD Eigenschaften Log On Fenster

Klicken Sie in den Kreis “Local System account”, **löschen Sie die Passwörter** ,und klicken Sie auf “Browse…”.

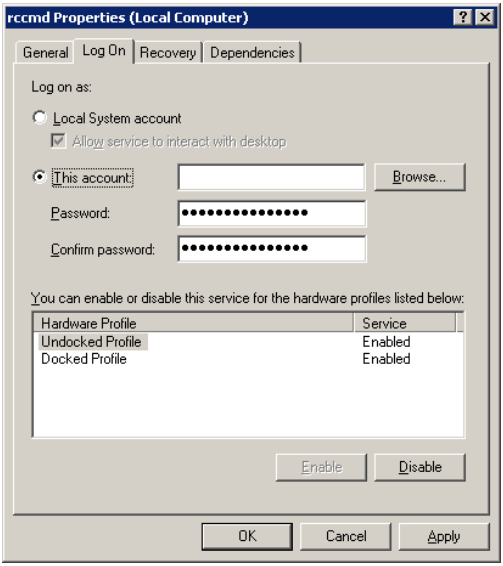

Abb. 46: RCCMD Eigenschaften Passwort-Bestätigung

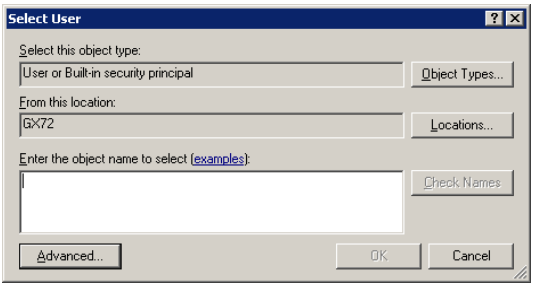

Abb. 47: Select User Fenster

Klicken Sie auf “examples”, um einen Objektnamen auszuwählen.

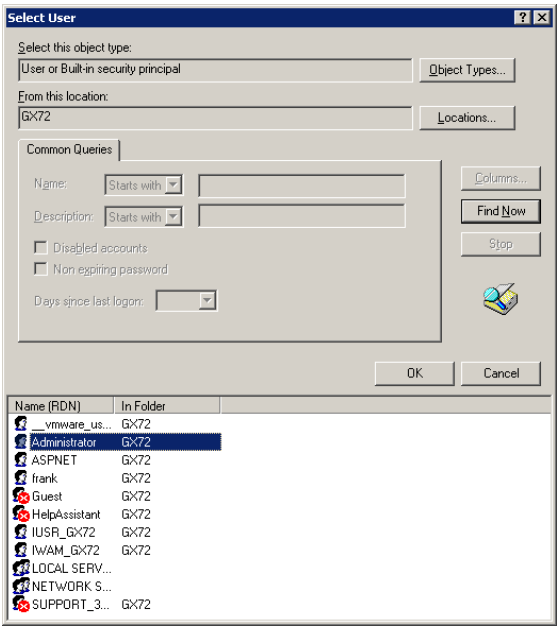

Abb. 48: Auswahl des Objektnamens

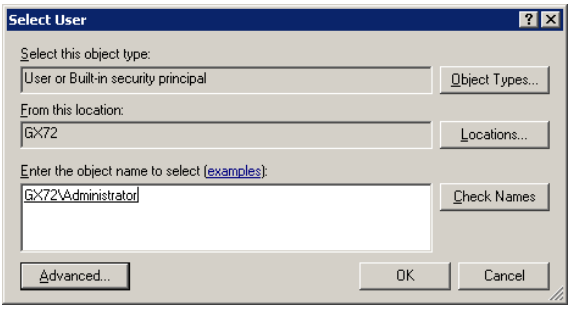

Abb. 49: Administrator Auswahl

Klicken Sie auf “Ok”, und tragen Sie das neue Passwort zweimal ein.

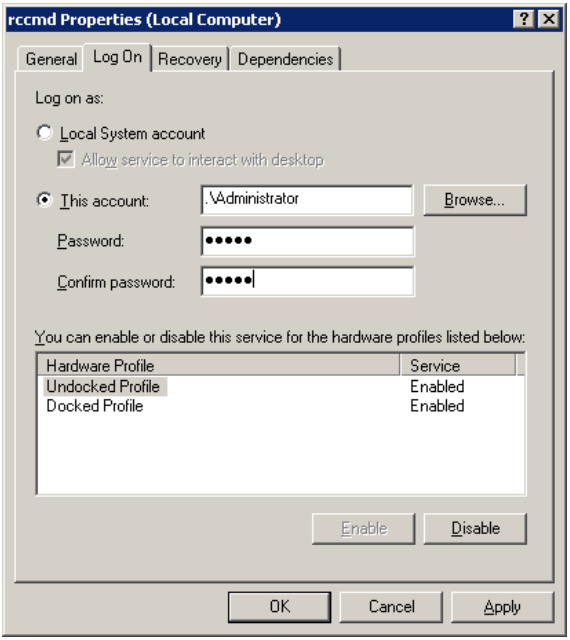

Abb. 50: Administrator Passwort Bestätigung

Abb. 51: Dienst-Berechtigungs-Fenster

2.7 Testen des Shutdown.Bat Files

Wir empfehlen Ihnen, das editierte Shutdown.Bat File zu testen. Das Shutdown Programm EXITWIN.EXE ist vordefiniert. Für die Syntax-Hilfe zu diesem Shutdown Tool, tippen Sie einfach RCCMD -? in dem RCCMD Verzeichnis. Sie können aber auch ein eigenes Shutdown Tool verwenden, das mit dieser Software kompatibel ist.

Achtung: **Wenn Ihre Konfiguration einwandfrei im Debug Modus läuft, bedeutet dies nicht gleichzeitig, dass es auch einwandfrei als RCCMD Windows NT Dienst funktioniert. Bitte vergewissern Sie sich, dass der RCCMD Dienst mit administrativer Berechtigung gestartet wurde, denn sonst könnte es passieren, dass nur uneingeschränkte Programme (z.B. notepad.exe) ausgeführt werden, aber keine Shutdowns (häufigste Fehlermeldung: "Adjust Token Privileges failed").**

Die komplette Befehls-Syntax für die NT-Konsole für RCCMD im Empfänger-Modus:

rccmd [–debug] -l [-a IP adress] [–h hostname] [-p port] "command"

Der Befehl kann ein Programm oder ein anderes Batch File auf dieser Workstation ausführen. Der Befehl sollte mit voller Pfadangabe eingegeben werden. Die "-p" Port Option kann eingefügt werden, wenn Sie RCCMD mehrmals auf einer Workstation ausführen möchten, um mehrere Befehle ausführen zu lassen. Der Standard Port ist 6003, benutzen Sie andere, freie Ports, um verschiedene Befehle auszuführen.

RCCMD in dem Sender Modus:

rccmd [–debug] -s [-a IP adress] [-h hostname] [-p port]

Dieser Befehl wird regelmässig in dem Batch File von dem Sender genutzt (shutdown.bat) und sendet ein Echosignal (ping) an die IP-Adresse der Workstation oder deren Hostnamen. Wenn das Echo beantwortet wurde, könnte der nächste Befehl ausgeführt werden (RCCMD –s) etc.

Wenn Sie die Editierung der Batch Files abgeschlossen haben, klicken Sie auf "Restart RCCMD".

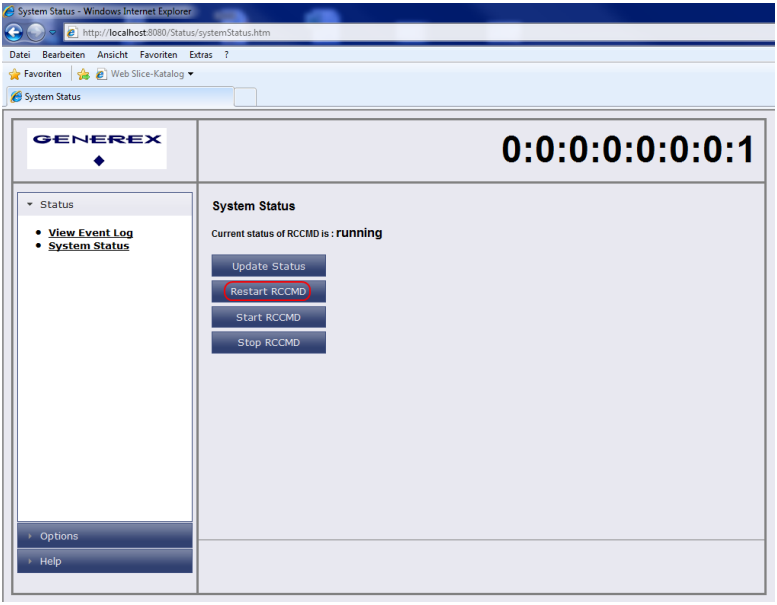

Abb. 52: System Status – Restart RCCMD

RCCMD läuft nun als Dienst mit automatischen Start. Um den automatischen Start zu konfigurieren, nutzen Sie die administrative Berechtigung, die Systemsteuerung und verändern Sie dort die Einstellungen in den Diensten.

WICHTIG: RCCMD als Dienst mit lokaler Desktop Interaktion ist in der Lage, lokale Shutdowns auszuführen. Um spezielle Aktionen via RCCMD durchzuführen, z.B. Starten einer NETSEND Nachricht oder andere Befehle, benötigt RCCMD extra Berechtigungen! Diese Berechtigungen werden in der Systemsteuerung/Dienste konfiguriert.

Senden einer Nachricht an alle RCCMD Clients

Um eine Nachricht an alle RCCMD Clients senden zu können, nutzen Sie bitte folgende Syntax:

rccmd –se “MSG_TEXT ups_says_hello_world” –a 192.9.200.255

Der RCCMD Client, der die Nachricht erhalten soll, muss entweder die IP-Adresse des Senders in seiner IP-Adressen-Liste eingetragen haben, oder die Liste muss leer sein. Da der CS121 nicht fähig ist, UDP-Broadcasts zu senden, muss man im RCCMD Client die o.g. Syntax eintragen, sodass der Client als Relay-Station die Nachricht weiterleitet. Von einem Windows-, UNIX- oder MAC OS-RCCMD Sender ist es kein Problem, diese Nachricht zu senden.

2.8 Testen der RCCMD Verbindung

Testen Sie letztendlich Ihre Konfiguration, wenn alle RCCMD Clients vorhanden sind. Führen Sie RCCMD im Debug Modus aus (RCCMD –debug –s/l-a). Senden Sie ein Echo (Ping) zu jedem Remote Client mit dem Befehl “ping [hostname][IP-Adresse]”. Wenn der Ping beantwortet wird, können Sie nun den RCCMD Verbindungs-Test im Debug-Modus starten. Wenn alles funktioniert, können Sie sehen, dass eine Verbindung aufgebaut und wieder geschlossen wurde. Das bedeutet, dass der Remote RCCMD Client Ihr Signal empfangen hat und das Shutdown script remote ausführen wird.

ACHTUNG! Dieser Test wird das Shutdown Script ausführen! Wenn Sie den Shutdown vermeiden möchten, sollten Sie den Shutdown-Befehl aus dem RCCMD Client Shutdown.Bat/SH File herausnehmen.

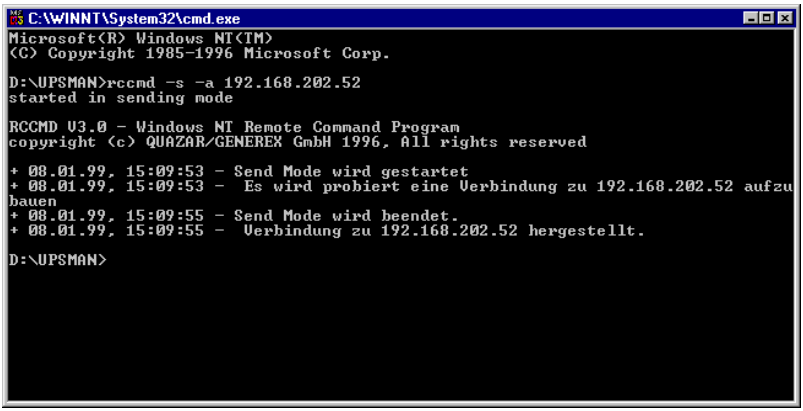
C:\WINNT\System32\cmd.exe
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.
D:\UPSMAN>rccmd -s -a 192.168.202.52
started in sending mode
RCCMD V3.0 - Windows NT Remote Command Program
copyright (c) QUAZAR/GENEREX GmbH 1996, All rights reserved
+ 08.01.99, 15:09:53 - Send Mode wird gestartet
+ 08.01.99, 15:09:53 - Es wird probiert eine Verbindung zu 192.168.202.52 aufzu
bauen
+ 08.01.99, 15:09:55 - Send Mode wird beendet.
+ 08.01.99, 15:09:55 - Verbindung zu 192.168.202.52 hergestellt.
D:\UPSMAN>

Abb. 53: RCCMD Konsolen-Test

2.8.1 Testen der RCCMD 2 Verbindung

Um zu überprüfen, ob der UPSMAN Prozess unter RCCMD 2 auf dem Remote Client aktiv ist, nutzen Sie folgende Syntax:

rccmd –sc –ac <IP address>

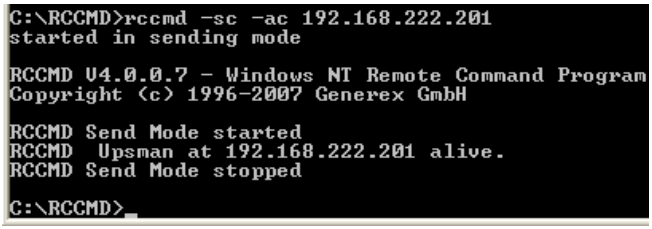
C:\RCCMD>rccmd -sc -ac 192.168.222.201
started in sending mode
RCCMD V4.0.0.7 - Windows NT Remote Command Program
Copyright (c) 1996-2007 Generex GmbH
RCCMD Send Mode started
RCCMD Upsman at 192.168.222.201 alive.
RCCMD Send Mode stopped
C:\RCCMD>

Abb. 54: RCCMD Alive Check via Befehlszeile

Wenn der UPSMAN aktiv ist, erhalten Sie die Nachricht “UPSMAN <IP-Adresse> alive”. Sie werden keine Nachricht erhalten, wenn der Dienst inaktiv ist.

Benutzen Sie diesen Befehl, um die RCCMD-Hilfe aufzurufen: C:\Program Files\RCCMD>rccmd -?

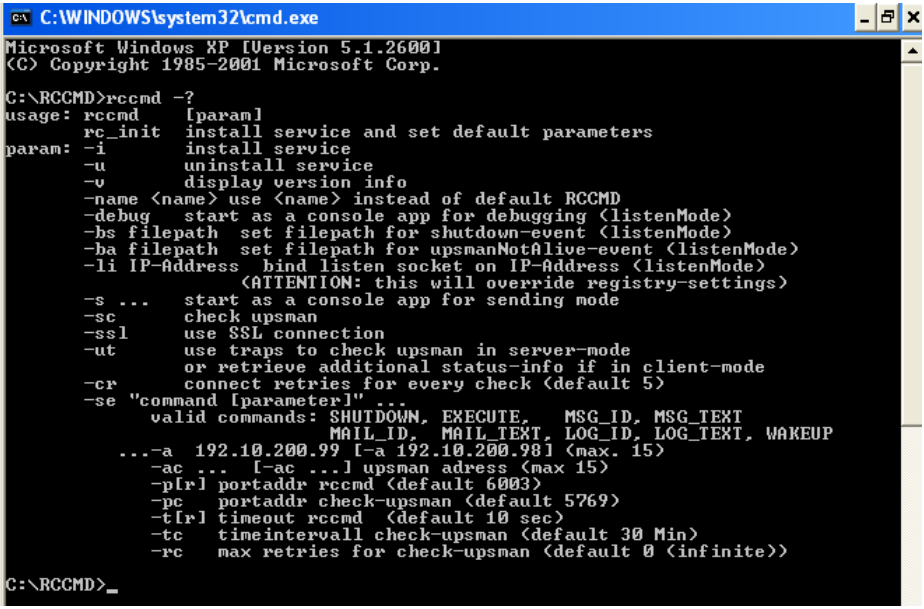
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\RCCMD>rccmd -?
usage: rccmd [param]
rc_init install service and set default parameters
param: -i install service
-u uninstall service
-v display version info
-name <name> use <name> instead of default RCCMD
-debug start as a console app for debugging (listenMode)
-bs filepath set filepath for shutdown-event (listenMode)
-ba filepath set filepath for upsmanNotAlive-event (listenMode)
-li IP-Address bind listen socket on IP-Address (listenMode)
(ATTENTION: this will override registry-settings)
-s ... start as a console app for sending mode
-sc check upsman
-ssl use SSL connection
-ut use traps to check upsman in server-mode
or retrieve additional status-info if in client-mode
-cr connect retries for every check (default 5)
-se "command [parameter]" ...
valid commands: SHUTDOWN, EXECUTE, MSG_ID, MSG_TEXT
MAIL_ID, MAIL_TEXT, LOG_ID, LOG_TEXT, WAKEUP
...-a 192.10.200.99 [-a 192.10.200.98] (max. 15)
-ac ... [-ac ...] upsman adress (max 15)
-p[r] portaddr rccmd (default 6003)
-pc portaddr check-upsman (default 5769)
-t[r] timeout rccmd (default 10 sec)
-tc timeintervall check-upsman (default 30 Min)
-rc max retries for check-upsman (default 0 (infinite))
C:\RCCMD>

Abb. 55: RCCMD Konsole -?

2.9 RCCMD auf Windows 95/98

RCCMD für Windows 95/98 funktioniert so, wie RCCMD auf Windows NT. Der einzige Unterschied ist der Programmname, nämlich RCCMD95.EXE. Bitte schauen Sie auch in den Windows Abschnitt von diesem Handbuch.

Achtung: **Für Windows 95/98 Benutzer empfehlen wir die Installation von dem TCP/IP Protokoll, bevor Sie die Installation des RCCMD Wizard starten.**

Achtung: **Wenn Sie WINPOP.EXE benutzen, können Sie RCCMD nicht auf dem Port 6003 starten. Bitte verändern Sie die Sender und Empfänger dementsprechend.**

Erfahrene Anwender sollten den Registry Editor nutzen und alle Veränderungen manuell vornehmen. Unerfahrene Anwender sollten den RCCMD Wizard benutzen.

Registry Einstellungen: Bitte überprüfen Sie Folgendes: Wenn Sie den RCCMD Prozess im Lauscher-Modus nutzen möchten, müssen Sie die folgenden Parameter in der Register Datenbank eintragen:

regedit.exe rccmd95.reg or simply start rc_init.bat

Die Parameter befinden sich nun im folgenden Register:

HKEY_LOCAL_MACHINE\CurrentControlSet\Services\RCCMD95\Parameters

Starten Sie die Regedit.Exe, wenn Sie RCCMD umkonfigurieren möchten.

Wenn Sie mit dem Register Editor von Windows 95 nicht vertraut sind, können Sie anstelle die RCCMD95.EXE modifizieren. Führen Sie die Regedit.Exe und die RCCMD.EXE aus:

Parameter:

***Port:* Spezieller TCP-Port, der das RCCMD Signal empfängt.**

***Addr1... 10*: TCP/IP Adresse von der Workstation, die das RCCMD Signal akzeptiert.**

***ExecutePrg*: Der Befehl, der beim empfang des RCCMD Signals ausgeführt wird.**

Um RCCMD zu starten, führen Sie diesen Befehl aus:

rccmd95

Oder starten Sie das Programm mit Hilfe der Startmenü-Leiste.

Um RCCMD im Sender Modus auszuführen, tragen Sie bitte die folgenden Parameter in Ihrem Shutdown-Job ein:

RCCMD95 -s -a <address> [-p 6003]

Mit <address> ist die IP-Adresse der Workstation gemeint, der Sie das RCCMD Signal senden möchten.

Optionale Parameter:

-p <port> = TCP-Port, zu dem das RCCMD Signal gesendet wird.

Die Option –a kann mehrere Male genutzt werden, wenn ein Shutdown auf mehreren Remote Computern ausgeführt werden soll.

Nutzen Sie die RCCMD CD-Lizenz nicht mehr als einmal (siehe Copyright, Seite 1). Wenn mehr als ein RCCMD Modul installiert werden muss, um einen Shutdown auszuführen, müssen Sie weitere Lizenzen bestellen, die Sie bei Ihrem USV Händler erhalten können.

2.10 RCCMD auf Windows NT/2000/XP/2003/2008

Das RCCMD (Remote Console Command) ist ein Programm, das die Ausführung von Programmen auf Remote Computer ermöglicht. Dieses Tool ist Teil von allen UPSMAN unterstützten Betriebssystemen, mit der Ausnahme von Windows 3.x. Dieses Tool bietet die Möglichkeit, Verbindungen zwischen verschiedenen Betriebssystemen herzustellen. Wenn die UPS Management Software auf einer Windows NT/2000/XP Maschine installiert

ist und ein Remote Shutdown auf einer Remote Maschine ausgeführt werden soll, auf dem ein anderes Betriebssystem läuft, werden Sie das RCCMD Tool benötigen.

Das RCCMD Tool arbeitet in zwei verschiedenen Modi. Das Modul arbeitet wie ein normales Programm, im Sender Modus, um RCCMD Befehle zu anderen Workstations zu senden, im Lauscher Modus, der als NT Dienst im Hintergrund läuft und auf Befehle wartet.

Achtung: **Für unerfahrene Anwender empfehlen wir das Ausführen des RCCMD Wizard, der die Konfiguration erleichtert. Starten Sie den Wizard von Ihrer entsprechenden Programm Gruppe.**

Attention: **Bitte benutzen Sie den Wizard und die Manuelle Konfiguration nicht zur gleichen Zeit.**

Eventuell benötigen Sie zum einwandfreien Ausführen von RCCMD besondere Privilegien, um Befehle und Programme auszuführen. Die RCCMD Start Parameter müssen in der Systemsteuerung auf den Administrator/Superuser mit dem korrekten Passwort eingetragen sein. Wenn Sie nicht authorisiert sind, den Admin Zugang zu benutzen, muss ein neuer Zugang eingerichtet werden, der die Berechtigung hat, diese Workstation herunterzufahren. Setzen Sie in der Systemsteuerung die RCCMD Start Parameter auf “This Account” und tragen Sie den “Any Administrative Account” ein.

Nun wurde RCCMD erfolgreich installiert und ist in der Lage, die C:\ups\shutdown.bat auszuführen.

2.11 RCCMD auf Windows 2008 Server Core x64

Bei der Konfiguration von RCCMD auf Windows 2008 Server Core x64 gibt es die Besonderheit, dass die RCCMD Konfiguration aus dem Standardverzeichnis C:\RCCMD mit dem folgenden Befehl aufzurufen ist:

```
C:\RCCMD>RCCNF_NT.EXE
```

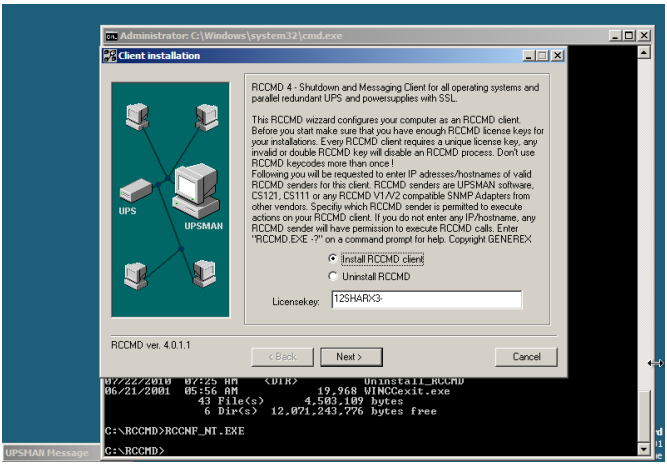
Administrator: C:\Windows\system32\cmd.exe
Client installation
RCCMD 4 - Shutdown and Messaging Client for all operating systems and parallel redundant UPS and powersupplies with SSL.
This RCCMD wizzard configures your computer as an RCCMD client. Before you start make sure that you have enough RCCMD license keys for your installations. Every RCCMD client requires a unique license key, any invalid or double RCCMD key will disable an RCCMD process. Don't use RCCMD keycodes more than once !
Following you will be requested to enter IP adresses/hostnames of valid RCCMD senders for this client. RCCMD senders are UPSMAN software, CS121, CS111 or any RCCMD V1/V2 compatible SNMP Adapters from other vendors. Specify which RCCMD sender is permitted to execute actions on your RCCMD client. If you do not enter any IP/hostname, any RCCMD sender will have permission to execute RCCMD calls. Enter "RCCMD.EXE -?" on a command prompt for help. Copyright GENEREX
Install RCCMD client
Uninstall RCCMD
Licensekey:
12SHARX3-
UPS
UPSMAN
RCCMD ver. 4.0.1.1
< Back
Next >
Cancel
06/21/2001 05:56 AM 19,968 WINCExit.exe
43 File(s) 4,503,109 bytes
6 Dir(s) 12,071,243,776 bytes free
C:\RCCMD>RCCNF_NT.EXE
C:\RCCMD>
UPSMAN Message

Abb. 56: RCCMD Konfiguration

Schauen Sie bitte in das Kapitel 2 für den Installationsablauf und in Kapitel 2.12 für die Konfiguration von RCCMD.

2.12 Alte RCCMD Konfiguration

Attention:

Im nachfolgenden Teil beschreiben wir die RCCMD Konfiguration anhand des bis 04/2012 verwendeten Windows Tools „Rccnf_nt.exe“. Alle Funktionen entsprechen der moderneren Variante von RCCMD WebInterface, welches ab 05/2012 verwendet wird (siehe Kapitel 4). Die detaillierten Funktionen sind Bediener-Interface unabhängig und werden im nachfolgenden Teil beschrieben.

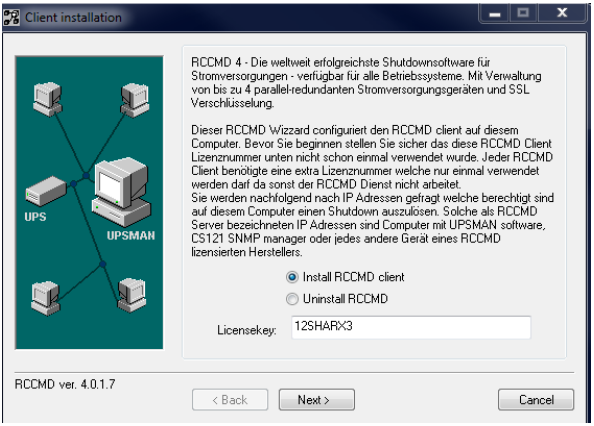
Client installation
RCCMD 4 - Die weltweit erfolgreichste Shutdownsoftware für Stromversorgungen - verfügbar für alle Betriebssysteme. Mit Verwaltung von bis zu 4 parallel-redundanten Stromversorgungsgeräten und SSL Verschlüsselung.
Dieser RCCMD Wizzard configuriert den RCCMD client auf diesem Computer. Bevor Sie beginnen stellen Sie sicher das diese RCCMD Client Lizenznummer unten nicht schon einmal verwendet wurde. Jeder RCCMD Client benötigte eine extra Lizenznummer welche nur einmal verwendet werden darf da sonst der RCCMD Dienst nicht arbeitet.
Sie werden nachfolgend nach IP Adressen gefragt welche berechtigt sind auf diesem Computer einen Shutdown auszulösen. Solche als RCCMD Server bezeichneten IP Adressen sind Computer mit UPSMAN software, CS121 SNMP manager oder jedes andere Gerät eines RCCMD lizensierten Herstellers.
Install RCCMD client
Uninstall RCCMD
Licensekey:
12SHARX3
UPS
UPSMAN
RCCMD ver. 4.0.1.7
< Back
Next >
Cancel

Abb. 57: Client Installation

Klicken Sie auf “Next”.

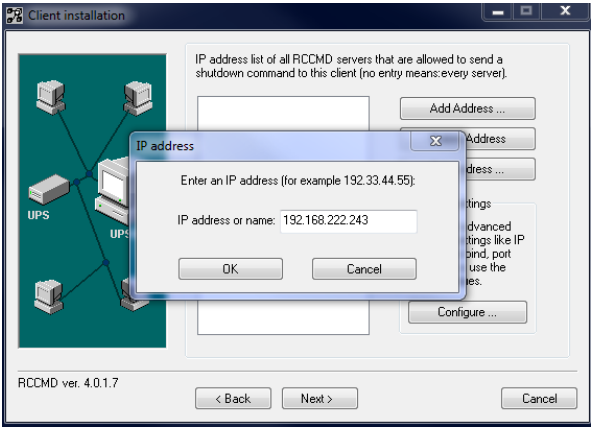
Client installation
IP address list of all RCCMD servers that are allowed to send a shutdown command to this client (no entry means:every server).
Add Address ...
IP address
Enter an IP address (for example 192.33.44.55):
IP address or name: 192.168.222.243
OK
Cancel
Configure ...
UPS
RCCMD ver. 4.0.1.7
< Back
Next >
Cancel

Abb. 58: Eingabe IP-Adresse

Step 4: Tragen Sie die IP-Adresse des RCCMD Servers ein, der authorisiert ist, ein Shutdown Signal zu senden.

Attention: **Wenn Sie hier keine Adresse eintragen, ist jeder Server in der Lage, einen Shutdown an diesen Client zu senden. Wenn mehr als ein CS121 oder UPSMAN in dem Netzwerk existieren, befinden Sie sich in der Redundanz Situation. Hier müssen mehrere Adressen als authorisierte Sender eingetragen werden.**

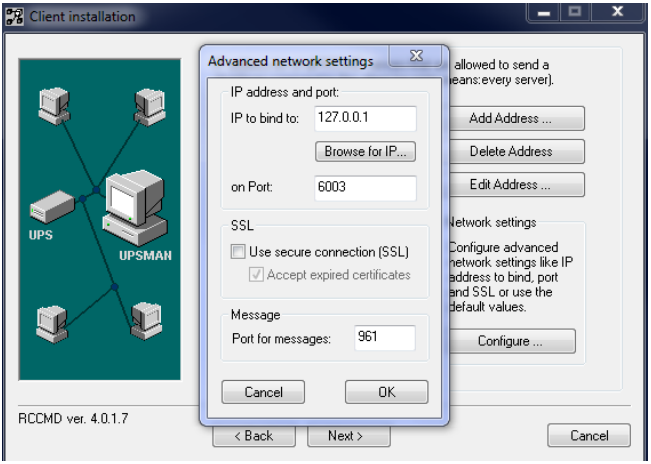

Abb. 59: Erweiterte Netzwerk Einstellungen

Step 5:

Wenn Sie eine SSL Verbindung nutzen möchten, klicken Sie auf “Configure…” und haken Sie die “SSL-Box” an, und es kann der Port für die Nachrichten verändert werden.

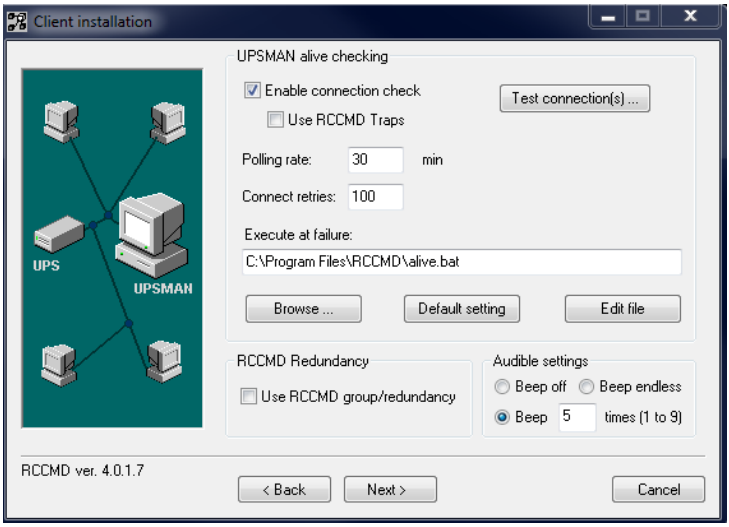

Abb. 60: UPSMAN Alive Checking / Redundanz Fenster

Step 6:

Wenn Sie die Funktion “UPSMAN Alive Checking” nutzen möchten (empfohlen), haken Sie die entsprechende Box an. Dieser Check ist ein Signal, das an den CS121 oder UPSMAN via Port 5769 gesendet wird, um zu prüfen, ob der UPSMAN noch USV Daten hat. Wenn nicht, wird das Script File “Alive.Bat” ausgeführt, das eine entsprechende Nachricht als Pop-Up bringt. Die Polling Rate (Standard 30 Minuten) definiert den Interval der UPSMAN Abfrage, connect retries (Verbindungswiederholungen, Standard 100) bedeutet, das nach 100 erfolglosen Verbindungsversuchen ein Alarm ausgelöst wird.

Die Funktion “Use RCCMD Traps” ermöglicht UPSMAN/RCCMD/UNMS Meldungen, die den USV Status als Nachricht anzeigen. Wenn aktiviert, wird diese Funktion eine lokale Nachricht bringen, wenn der USV Status des UPSMAN/RCCMD Servers sich verändert.

Wenn Sie auf “Test connections…” klicken, wird das UPSMAN Alive Checking von der eingetragenen IP-Adresse gestartet (der Port 5769 wird getestet).

Unter „Audible Settings“ können die Toneinstellungen der RCCMD Nachrichtenbox definiert werden.

- **Beep off:** Ton aus
- **Beep endless:** Ton endlos
- **Beep:** Definition Anzahl der Pieptöne (1 bis 9)

Wenn Sie auf “Browse…” klicken, werden Sie eine Auswahl der Standard Batch Files erhalten.

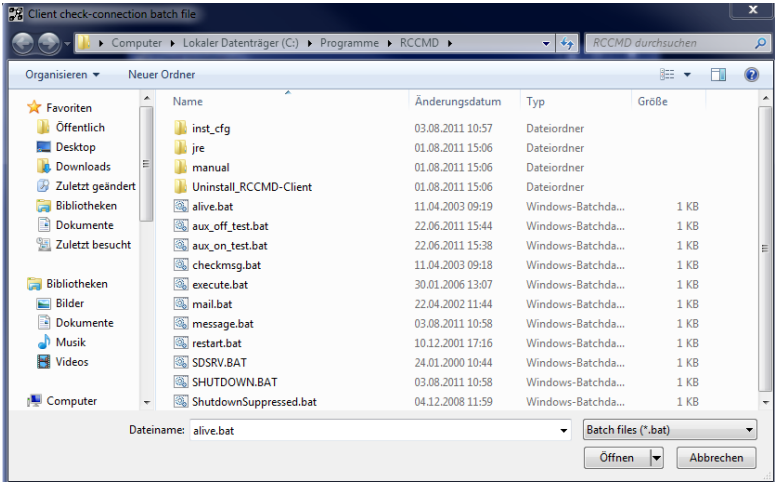

Abb. 61: Client Check Connection Batch File Fenster

Wenn Sie auf „Default Setting“ klicken, werden Sie zurück zum Alive.Bat File gelangen.

Bei einem Fehler von dem UPSMAN Alive Check können Sie eine auszuführende Datei konfigurieren oder das Standard File “Alive.Bat” editieren:

@echo off

rem * "messagetext" %1 == ip-address, %2 == date, %3 == time *** "title" -c counter for beeps**

start /b msg.exe "Check Upsman %1 failed (%2, %3)" "ATTENTION RCCMD:" -c:1

Klicken Sie auf “Next”.

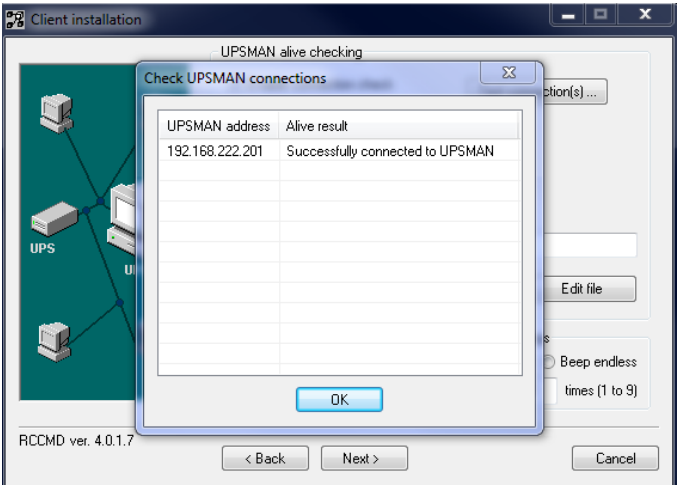

Abb. 62: Check UPSMAN Connections Fenster

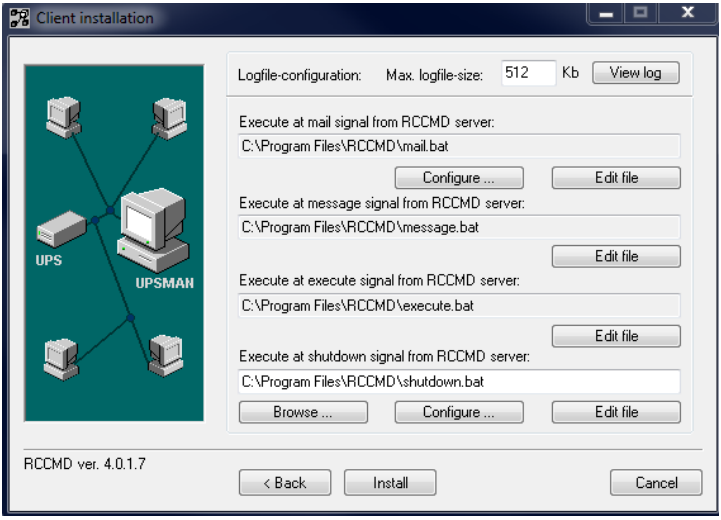

Abb. 63: Konfiguration der Batch Files Fenster

Step 7: Sie können die Log File Grösse konfigurieren und die auszuführenden Bat Files editieren.

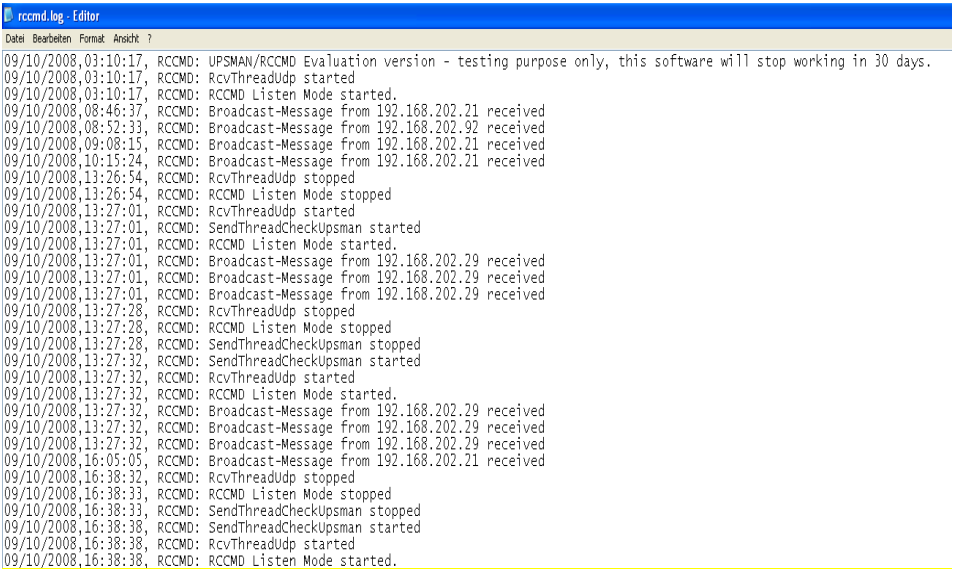
rccmd.log - Editor
Datei Bearbeiten Format Ansicht ?
09/10/2008,03:10:17, RCCMD: UPSMAN/RCCMD Evaluation version - testing purpose only, this software will stop working in 30 days.
09/10/2008,03:10:17, RCCMD: RcvThreadUdp started
09/10/2008,03:10:17, RCCMD: RCCMD Listen Mode started.
09/10/2008,08:46:37, RCCMD: Broadcast-Message from 192.168.202.21 received
09/10/2008,08:52:33, RCCMD: Broadcast-Message from 192.168.202.92 received
09/10/2008,09:08:15, RCCMD: Broadcast-Message from 192.168.202.21 received
09/10/2008,10:15:24, RCCMD: Broadcast-Message from 192.168.202.21 received
09/10/2008,13:26:54, RCCMD: RcvThreadUdp stopped
09/10/2008,13:26:54, RCCMD: RCCMD Listen Mode stopped
09/10/2008,13:27:01, RCCMD: RcvThreadUdp started
09/10/2008,13:27:01, RCCMD: SendThreadCheckUpsman started
09/10/2008,13:27:01, RCCMD: RCCMD Listen Mode started.
09/10/2008,13:27:01, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:01, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:01, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:28, RCCMD: RcvThreadUdp stopped
09/10/2008,13:27:28, RCCMD: RCCMD Listen Mode stopped
09/10/2008,13:27:28, RCCMD: SendThreadCheckUpsman stopped
09/10/2008,13:27:32, RCCMD: SendThreadCheckUpsman started
09/10/2008,13:27:32, RCCMD: RcvThreadUdp started
09/10/2008,13:27:32, RCCMD: RCCMD Listen Mode started.
09/10/2008,13:27:32, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:32, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:32, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,16:05:05, RCCMD: Broadcast-Message from 192.168.202.21 received
09/10/2008,16:38:32, RCCMD: RcvThreadUdp stopped
09/10/2008,16:38:33, RCCMD: RCCMD Listen Mode stopped
09/10/2008,16:38:33, RCCMD: SendThreadCheckUpsman stopped
09/10/2008,16:38:38, RCCMD: SendThreadCheckUpsman started
09/10/2008,16:38:38, RCCMD: RcvThreadUdp started
09/10/2008,16:38:38, RCCMD: RCCMD Listen Mode started.

Abb. 64: RCCMD Log File

Step 8: Wenn Sie via RCCMD Emails versenden möchten, klicken Sie auf „Configure…“.

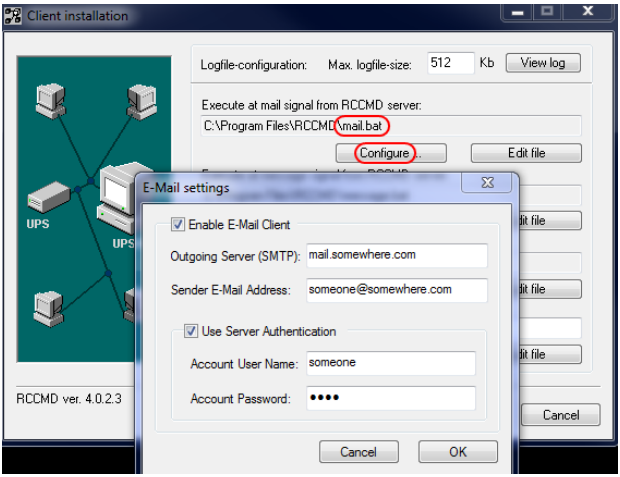

Abb. 65: RCCMD Email Settings

Geben Sie die entsprechenden Parameter ein, und klicken Sie auf „OK“. Das RCCMD Kommando zum Versenden einer Email lautet: mail Empfänger Adresse Text.

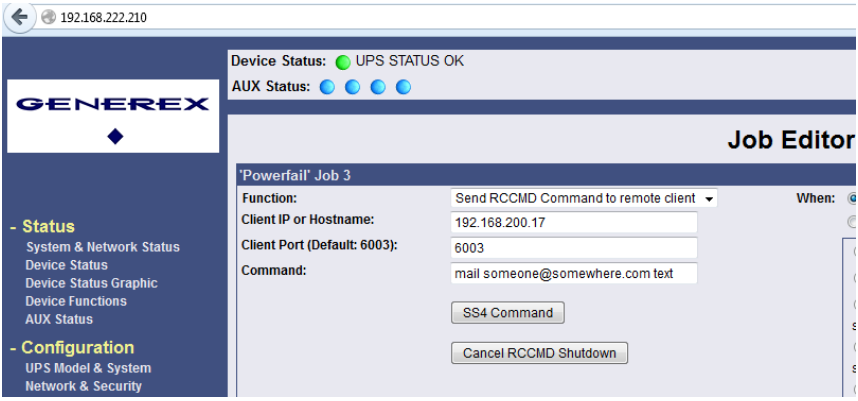

Abb. 66: CS121 Email Kommando

Step 9: Wenn Sie die Shutdown Sequenz verändern möchten, klicken Sie auf „Configure…“.

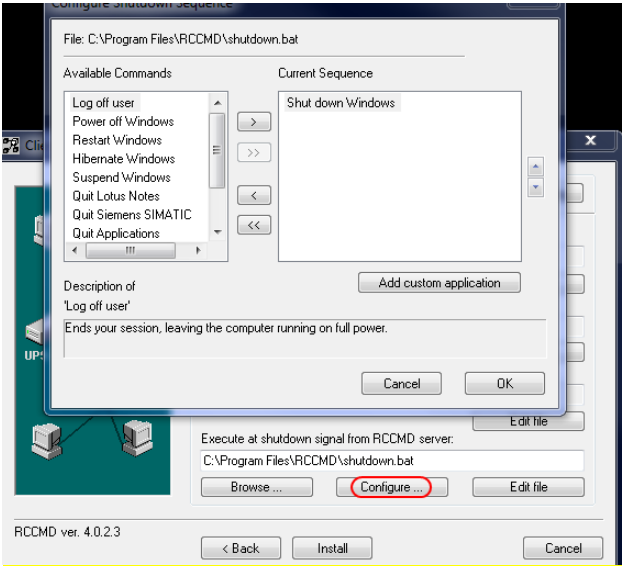

Abb. 67: RCCMD Shutdown Sequenz Konfiguration

2.12.1 Der RCCMD Client als Relay Station

Wenn Sie eine grössere Anzahl von RCCMD Empfänger erreichen möchten, muss ein RCCMD Client als Relay Station fungieren. Der Empfänger wird so konfiguriert, dass er beim Erhalten eines RCCMD Signals eine Batch Datei startet, die weitere RCCMD Signale versendet. Diese Workstation ist dann Empfänger und Sender zur gleichen Zeit und somit eine wichtige Verbindung in der USV Überwachungskette. Der Gebrauch von einem RCCMD Client als Relay Station macht die Überwachung von mehreren hundert

RCCMD Clients sehr viel einfacher als die Konfiguration über das Web-Interface des CS121. Außerdem haben alle Webbrowser Event Konfigurationen eine Sicherheits-limitierung, sodas es erforderlich ist, diese Relay Funktion zu nutzen, wenn die Anzahl der Jobs 50 pro Event auf dem CS121 HW131 übersteigt.

Sehen Sie in das folgende Script, das den RCCMD Client als Relay Station agieren lässt:

```
rem created by setup
@echo off
set path=%path%;C:\Program Files\RCCMD
# RELAY RCCMD
# This batch will send RCCMD shutdowns to the IP addresses listed below
# At the end of the batch this computer will initiate the local shutdown
start rccmd -s -a 192.168.200.2
start rccmd -s -a 192.168.200.3
start rccmd -s -a 192.168.200.4
start rccmd -s -a 192.168.200.5
start rccmd -s -a 192.168.200.6
start rccmd -s -a 192.168.200.7
# to be continued
#
# local shutdown
ExitWin.exe shutdown force
@cls
```

Abb. 68: Example: Batch File RCCMD als Relay Station

„start“ ist ein Windows Batchfile Kommando, um ein Programm-Aufruf in mehreren Instanzen zu starten. Dies ermöglicht das Ausführen von Programmen simultan und beschleunigt die Shutdown-Prozedur. Bitte beachten Sie, dass „start“ nicht auf allen Windows OS unterstützt wird und sollte getestet werden, bevor es verwendet wird.

Ab der RCCMD Version 4.0.1.0 ist auch eine grafische Konfiguration im RCCMD Wizard für die Relay Funktion enthalten.

Klicken Sie in der Client Installation auf “Configure…”.

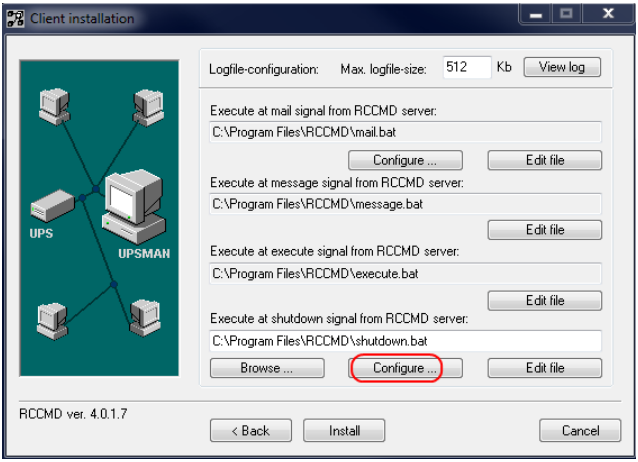

Abb. 69: RCCMD Client Shutdown Konfiguration

Markieren Sie im “Available Commands” Fenster das “RCCMD shutdown relay”, und klicken Sie auf den Pfeil “>”, um diese Funktion der “Current Sequence” hinzuzufügen.

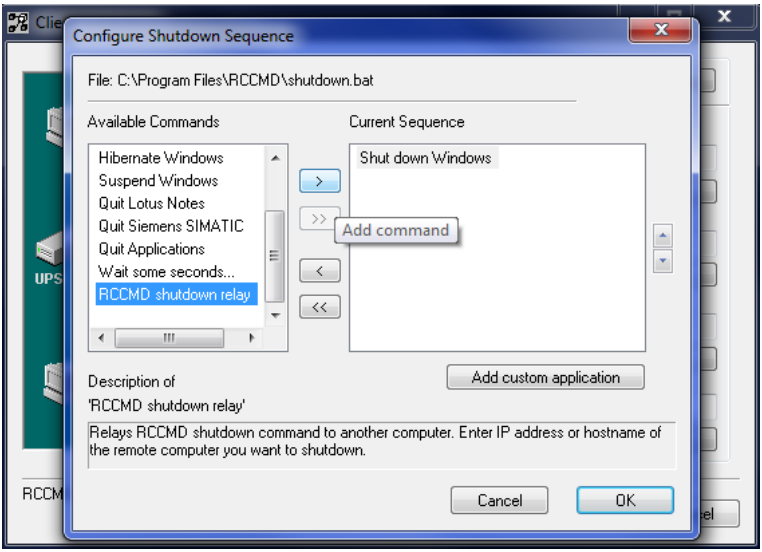

Abb. 70: RCCMD Shutdown Relay

Es öffnet sich das folgende Fenster, in dem man den gewünschten IP-Adressen-Bereich eingeben kann oder eine einzelne IP-Adresse.

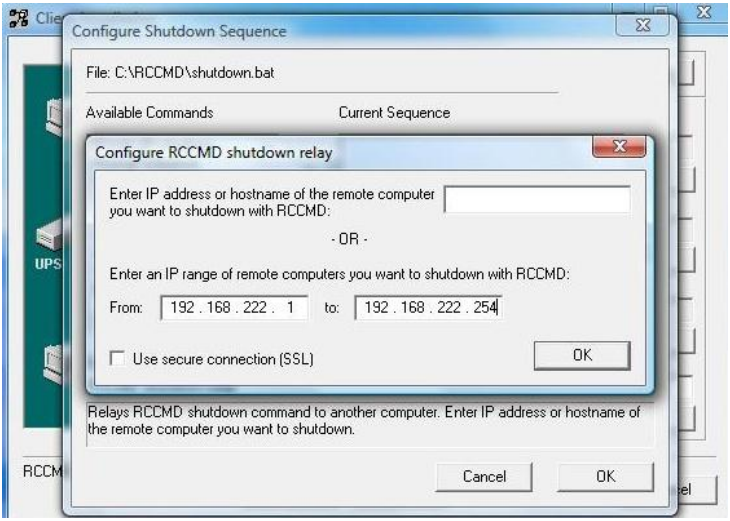
Configure Shutdown Sequence
File: C:\RCCMD\shutdown.bat
Available Commands
Current Sequence
Configure RCCMD shutdown relay
Enter IP address or hostname of the remote computer you want to shutdown with RCCMD:
- OR -
Enter an IP range of remote computers you want to shutdown with RCCMD:
From:
192 . 168 . 222 . 1
to:
192 . 168 . 222 . 254
Use secure connection (SSL)
OK
Relays RCCMD shutdown command to another computer. Enter IP address or hostname of the remote computer you want to shutdown.
Cancel
OK

Abb. 71: RCCMD Konfiguration IP-Adressen-Bereich

Ausserdem kann man hier auch die SSL-Funktion aktivieren (siehe auch Kapitel 3.9).

Um einzelne IP-Adressen aus dem Bereich zu entfernen, markieren Sie die Zeile mit der gewünschten Adresse, und klicken Sie auf den Pfeil “<”.

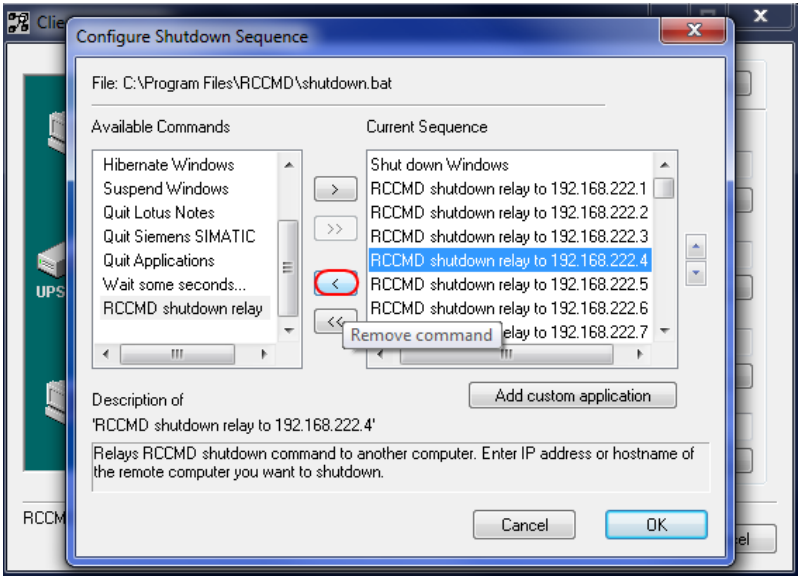

Abb. 72: RCCMD Shutdown Relay Adress-Entfernung

Das Ergebnis der grafischen Konfiguration von einem RCCMD Relay befindet sich in dem Shutdown-Skriptfile „shutdown.bat“.

```
@ECHO off
REM --- Created by RCCMD configuration ---
SET path=%path%;C:\Program Files\RCCMD
rccmd.exe -s -a 192.168.200.10
rccmd.exe -s -a 192.168.200.11
rccmd.exe -s -a 192.168.200.12
rccmd.exe -s -a 192.168.200.13
rccmd.exe -s -a 192.168.200.14
rccmd.exe -s -a 192.168.200.15
rccmd.exe -s -a 192.168.200.16
rccmd.exe -s -a 192.168.200.17
rccmd.exe -s -a 192.168.200.18
rccmd.exe -s -a 192.168.200.19
rccmd.exe -s -a 192.168.200.20
ExitWin.exe shutdown force
@CLS
```

Abb. 73: RCCMD Shutdown Relay in der „Shutdwown.bat“

Der Unterschied zu der o.g. Beschreibung der Shutdown-Sequenz ist, dass das grafische Tool nicht den „start“ Parameter verwendet und dadurch der Shutdown die Signale nacheinander versendet. Jede IP-Adresse, die auf diesen RCCMD Call nicht antwortet, benötigt 10 Sekunden (default) bis der Timeout erreicht ist und das nächste Kommando ausgeführt wird.

3. RCCMD auf UNIX (mit grafischer Oberfläche)

Das RCCMD (Remote Console Command) ist ein Programm, das die Ausführung von Programmen auf Remote Computer ermöglicht. Dieses Tool ist Teil von allen UPSMAN unterstützten Betriebssystemen sowie aller GENEREX CS121 SNMP Manager, BACS WEBMANAGER oder RCCMD lizensierten SNMP Managern anderer Hersteller (z. B. RITTAL CMC, GENERAL ELECTRIC SNMP, CHLORIDE-MASTERGAURD usw.).

Das RCCMD Tool basiert auf dem TCP/IP Protokoll und arbeitet in zwei verschiedenen Modi. Das Modul arbeitet wie ein normales Programm, im Sender Modus, um RCCMD Befehle zu anderen Workstations zu senden, im Lauscher Modus, der als UNIX Daemon im Hintergrund läuft und auf Befehle wartet.

Hinweis:

Der RCCMD Installer verwendet die von uns mitgelieferte Java Runtime Version, die nur für die Installation bzw. Deinstallation verwendet wird. Zusätzlich verwendet der RCCMD Web Configurator einen Java Webserver (jetty). Den RCCMD Web Configurator kann man entweder aus dem Autostart (/etc/init.t/rccmdConfig) entfernen oder den Symlink /usr/rccmd/runRccmdConfig umbenennen. Dann verwendet RCCMD kein Java mehr!

ACHTUNG: Wenn Sie ein OS ohne grafische Oberfläche nutzen, schauen Sie bitte in die FAQs, wie man z.B. einen USB-Stick mounted.

3.1 RCCMD Installation auf UNIX OS

RCCMD muss als user root von einer rootshell oder grafischen Terminal installiert werden. Dazu extrahieren Sie die Datei **rccmd.tar**, kopieren Sie nach z. B. */temp*, dann Start des Programms **rccmd.bin**. Es startet die folgende, grafische Installation:

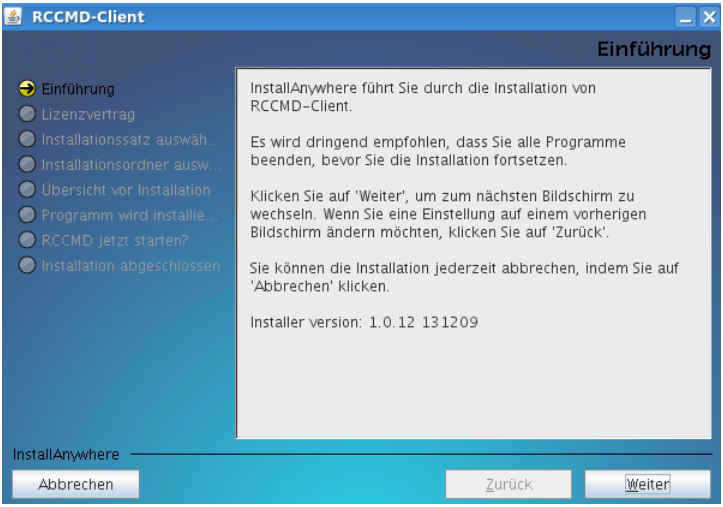
RCCMD-Client
Einführung
Einführung
Lizenzvertrag
Installationssatz auswäh...
Installationsordner ausw...
Übersicht vor Installation
Programm wird installie...
RCCMD jetzt starten?
Installation abgeschlossen
InstallAnywhere führt Sie durch die Installation von RCCMD-Client.
Es wird dringend empfohlen, dass Sie alle Programme beenden, bevor Sie die Installation fortsetzen.
Klicken Sie auf 'Weiter', um zum nächsten Bildschirm zu wechseln. Wenn Sie eine Einstellung auf einem vorherigen Bildschirm ändern möchten, klicken Sie auf 'Zurück'.
Sie können die Installation jederzeit abbrechen, indem Sie auf 'Abbrechen' klicken.
Installer version: 1.0.12 131209
InstallAnywhere
Abbrechen
Zurück
Weiter

Abb. 74: Installation – Einführung

Es folgt die Eingabe des Lizenzschlüssels.

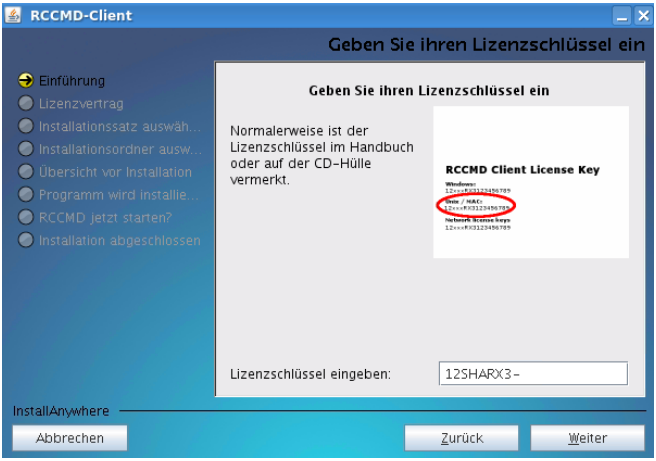

Abb. 75: Installation – Lizenzeingabe

Wählen Sie die gewünschten Features aus.

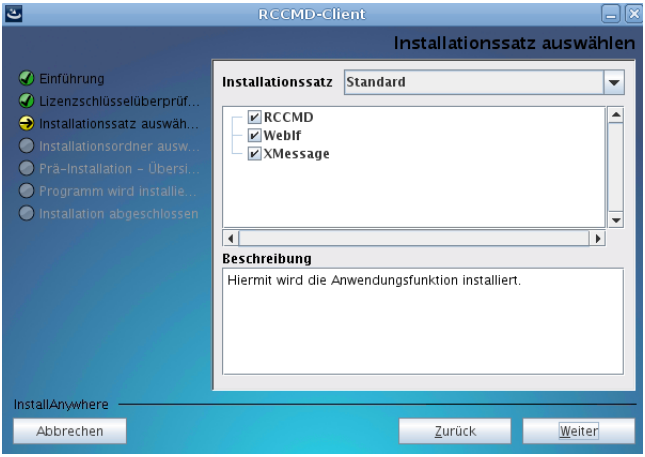

Abb. 76: Installation – Installationssatz Auswahl

Wählen Sie den gewünschten Installations-Pfad.

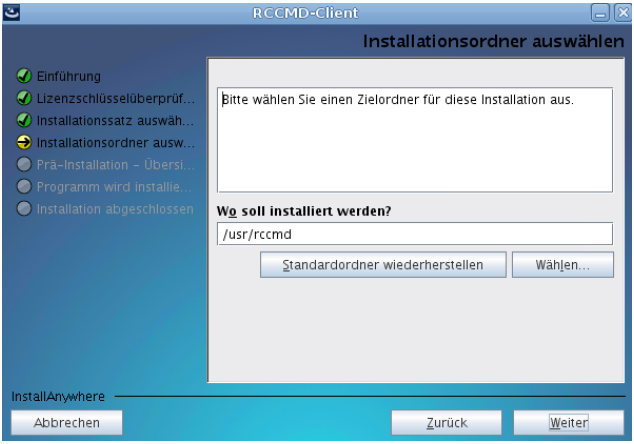

Abb. 77: Installation – Ordnerauswahl

Im nächsten Fenster können Sie die Options-Auswahl für die RCCMD Nachrichten treffen.

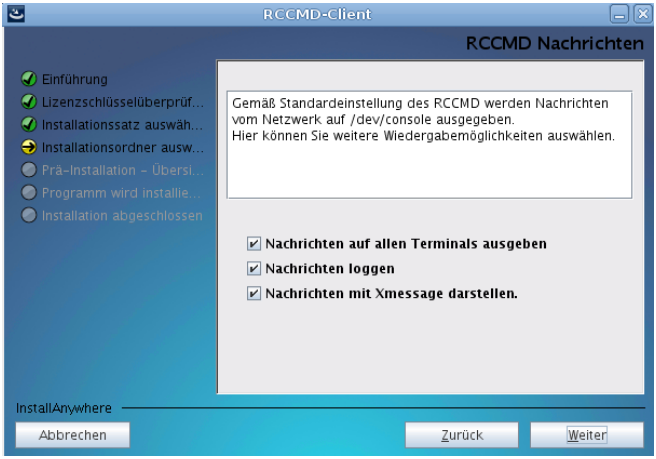

Abb. 78: Installation – Auswahl der Wiedergabemöglichkeiten

Es folgt die Zusammenfassung der Installation.

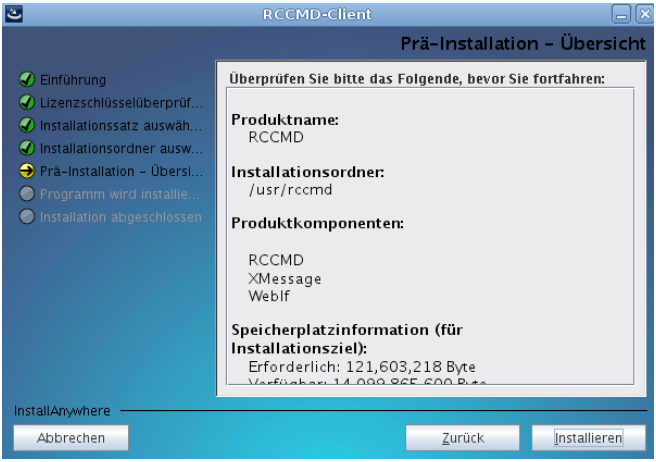

Abb. 79: Installation – Prä-Installations-Übersicht

Klicken Sie auf „Installieren“, um die Installation zu starten.

Im nächsten Fenster können Sie die Standardeinstellungen für den Web-Interface Zugriff akzeptieren oder ändern

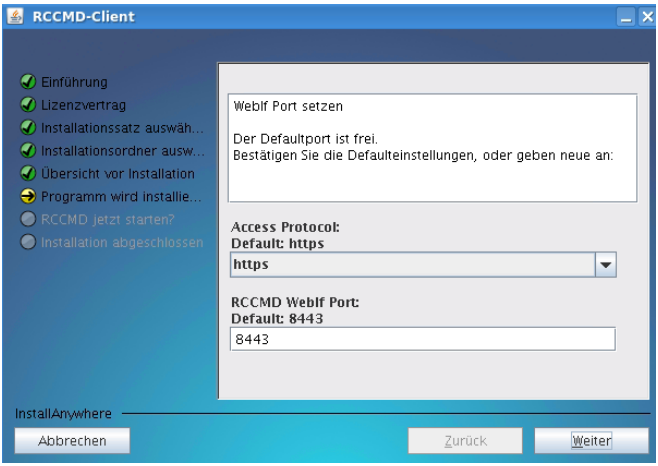

Abb. 80: Installation – Auswahl RCCMD Weblf Zugriff

Im nächsten Fenster werden die notwendigen Firewall Ausnahmen aufgelistet. Bitte schalten Sie diese Ports in Ihrer Firewall frei.

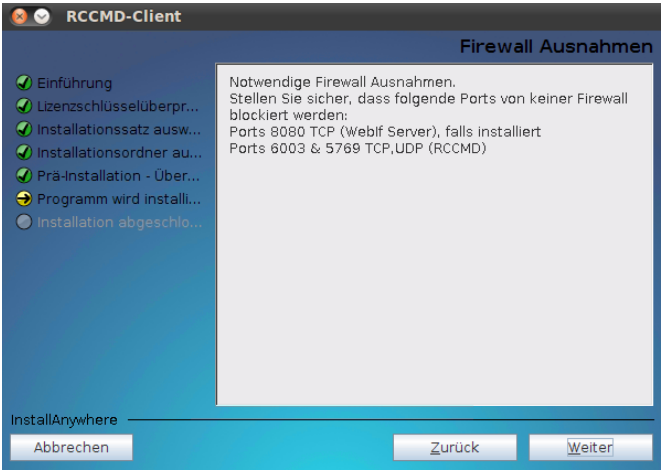

Abb. 81: Installation – Firewall Ausnahmen

In diesem Menü kann das Standardpasswort verändert werden.

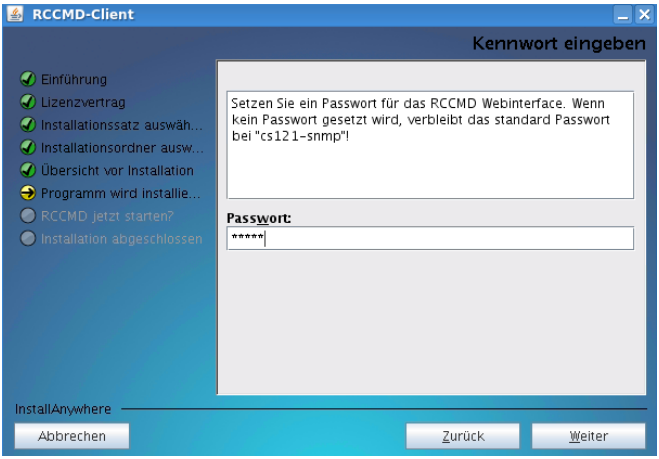

Abb. 82: Installation – Kennworteingabe

Zusätzlich kann ein Passworthinweis eingegeben werden.

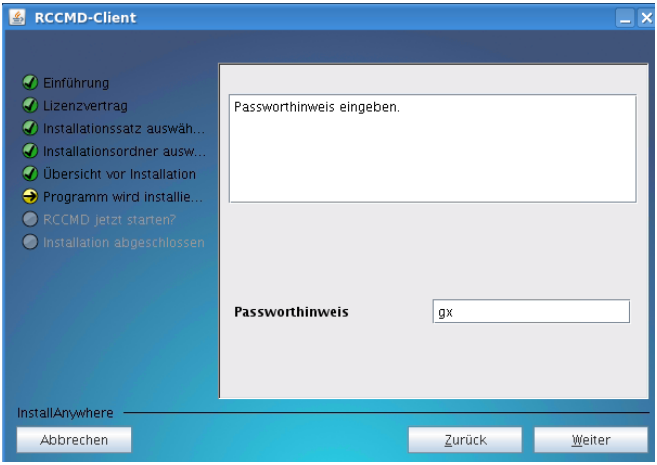

Abb. 83: Installation – Passworthinweis-Eingabe

Es folgt ein Hinweis, dass eine Konfiguration der RCCMD Software erforderlich ist.

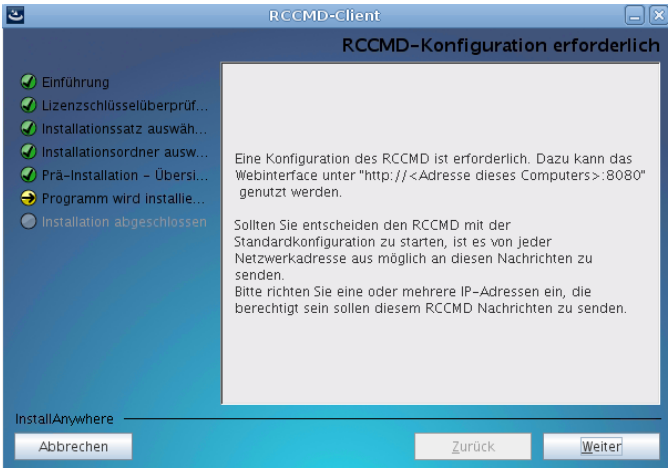
RCCMD-Client
RCCMD-Konfiguration erforderlich
Einführung
Lizenzschlüsselüberprüf...
Installationssatz auswäh...
Installationsordner ausw...
Prä-Installation - Übersi...
Programm wird installie...
Installation abgeschlossen
Eine Konfiguration des RCCMD ist erforderlich. Dazu kann das Webinterface unter "http://<Adresse dieses Computers>:8080" genutzt werden.
Sollten Sie entscheiden den RCCMD mit der Standardkonfiguration zu starten, ist es von jeder Netzwerkadresse aus möglich an diesen Nachrichten zu senden.
Bitte richten Sie eine oder mehrere IP-Adressen ein, die berechtigt sein sollen diesem RCCMD Nachrichten zu senden.
InstallAnywhere
Abbrechen
Zurück
Weiter

Abb. 84: Installation – Konfigurations-Hinweis

Es folgt ein RCCMD Start Hinweis.

Abb. 85 Installation – RCCMD Start Hinweis

Damit ist die Installation erfolgreich beendet.

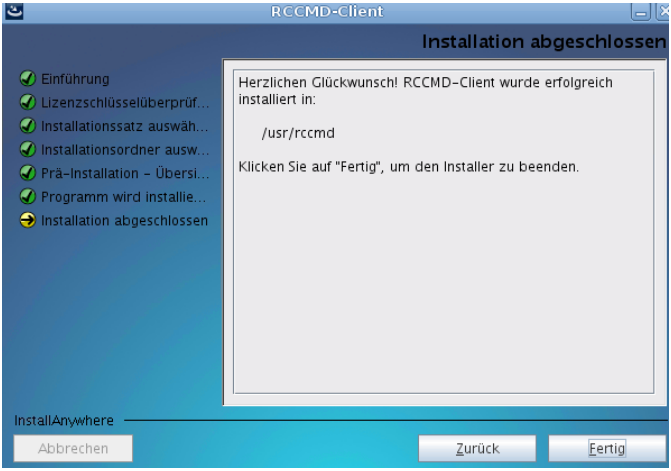

Abb. 86: Installation – Abschluss

3.2 Silent Installation für die RCCMD Installation auf UNIX OS

Eine „Silent Installation“ ist eine automatisierte Installations-Prozedur, wo die Benutzerdaten von einem File empfangen werden. Dies ermöglicht die Software Installation ohne Eingaben vom Anwender oder einer grafischen Schnittstelle.

In der RCCMD Software besteht die Möglichkeit, eine Silent Installation (Automatisiert Hintergrundinstallation ohne Benutzerinput) zu aktivieren. Bevor man diese Funktion nutzen möchte, sind Einstellungen in der Datei „installer.properties“ notwendig. Diese befindet sich auf der UPS Management CD im Verzeichnis \Rccmd\Linux\12.

This file provides Values to alter the behaviour of the installer.

You can preset Values for some internal Variables.

For the installer to find and use this file it is necessary to either rename

this file or pass a parameter to the installer when calling it.

If this file is called 'installer.properties' or has the same name as the

installer, e.g. 'install_RCCMD.properties' then the installer should

automatically use this file.

To call the installer with a parameter providing a properties file, the

installer need the parameter '-f' in this case the command line call looks

somewhat like this: "install_RCCMD.exe -f silent-installer.properties".

To set the installer User Interface without providing the variable in the

properties file, the parameter '-i' can be used.

```
##  E.g. "install_RCCMD.exe -i silent"
##  The interface options are "silent,gui,console" the gui option is default.
## Choose Feature List
## --------------------
## If you want to install a subset of features from this installer,
##  make a list of all the features you want to be installed.
## The List must be entered in the CHOSEN_INSTALL_FEATURE_LIST variable.
## Options for the list are: RCCMD, WebIf,XMessage
## CHOSEN_INSTALL_FEATURE_LIST=RCCMD,WebIf,XMessage
## This will set the User Interface of the installer
## For installation in console modus, pass the parameter: "-i console" to
## the installer.
#INSTALLER_UI=silent
## This presets the Licensekey. This value is necessary for a silent
##  installation, because there is no other way to pass this information to
##  the installer.
#GXLICENSEKEY=
## The Dialogbutton variable contains the answer to the pop-up question whether
##  the RCCMD should be started at system boot.
##  The value '0' (default) resembles the answer 'Yes' the value '1' corresponds
##  to 'no'.
#CHOSEN_DIALOG_BUTTON=0
## This variable decides whether RCCMD is started after installer ends. Use with care!
## RCCMD should be configured before it is started!
## '0' resembles the answer 'Yes' the value '1' (default) corresponds
##  to 'no'.
#CONSOLE_START_RCCMD_NOW=1
## Select the language for the installed version of RCCMD by setting the
```

```
##  INST_LANG variable to the desired country-code
##  (e.g.: el,en,es,de,fr,he,it,ja,ko,pt,ru,tr,zh_cn).
#INST_LANG=en
## Select the destination where the program should be installed
#USER_INSTALL_DIR=/usr/rccmd
## If the target System is a vSphere Management Assistant (vMA)
##  please provide the name or IP for the ESXi host.
#ESXI_HOST=127.0.0.1
## WebIf Settings
## --------------
## Here you can override default settings for access to the RCCMD WebIf.
## These settings are ignored, if the variable CHOSEN_INSTALL_FEATURE_LIST
## is set and does not contain the WebIf feature.
## In interactive install modes (gui, console) the installer will check, whether
## the chosen port is free to be used.
## Valid values are: 1-65535
## WEBIF_PORT=8080
## Valid protocols are: http, https
## WEBIF_PROTOCOL=http
```

Abb. 80: Dateiinhalt „installer.properties“

Um die Silent Installation zu aktivieren, müssen Sie das Doppelkreuz vor der Variabel `INSTALLER_UI=silent` entfernen. Zusätzlich ist die Eingabe eines Lizenzschlüssels hinter der Variabel `GXLICENSEKEY=` erforderlich. Führen Sie die „installRCCMD.bin“ als root aus.

Weitere Optionen sind: `INSTALLER_UI=console` für die interaktive Installation ohne grafische Schnittstelle oder `INSTALLER_UI=console`, um die grafische Installation zu nutzen (Standard).

3.3 Console Installation für die RCCMD Installation auf UNIX OS

Eine Konsolen-Installation ist notwendig, wenn Ihr Zielsystem keine grafische Oberfläche für die Ausführung des „installRCCMD.bin“ besitzt. Diese Konsolen-Installation arbeitet interaktiv und wird die im „installer.properties“ aufgeführten Fragen auf der Konsole ausgeben, die der Benutzer beantworten muss.

Hinweis: Dies betrifft nur die Installation, die Konfiguration wird mittels Editor in der Datei „rccmd.cfg“ ausgeführt.

Um die Console Installation zu aktivieren, müssen Sie das Doppelkreuz vor der Variabel `INSTALLER_UI=` entfernen und `console` eintragen. Dies ist die interaktive RCCMD Installation auf der Konsole. Führen Sie als *root* die „installRCCMD.bin“ aus.

Die Sprachauswahl können Sie mit der Variabel INST_LANG=de treffen, damit Ihnen bei der Konfiguration von der RCCMD Software die Tooltipps in der gewünschten Sprache zur Verfügung stehen.

3.3.1 Beispiel einer Console Installation

Ändern Sie die Datei „installer.properties“ entsprechend wie oben beschrieben ab, oder führen Sie einfach den Befehl **./installRCCMD.bin –i console** aus.

Wählen Sie die gewünschte Sprache aus, und beachten Sie die Einführung.

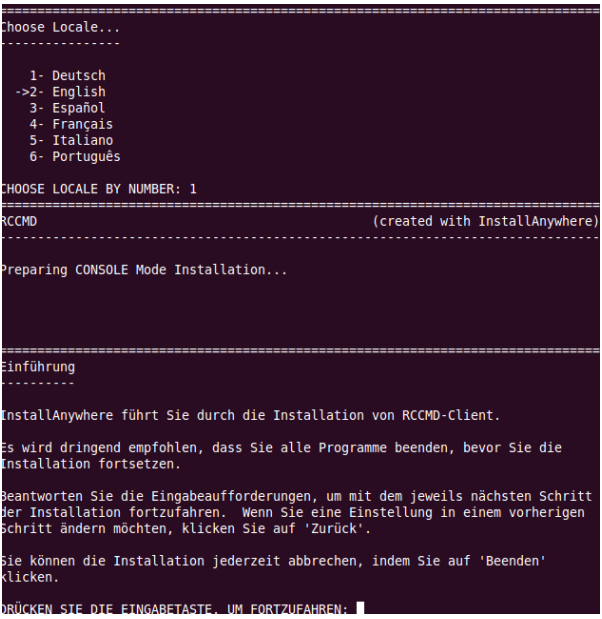
Choose Locale...
1- Deutsch
->2- English
3- Español
4- Français
5- Italiano
6- Português
CHOOSE LOCALE BY NUMBER: 1
RCCMD
(created with InstallAnywhere)
Preparing CONSOLE Mode Installation...
Einführung
InstallAnywhere führt Sie durch die Installation von RCCMD-Client.
Es wird dringend empfohlen, dass Sie alle Programme beenden, bevor Sie die Installation fortsetzen.
Beantworten Sie die Eingabeaufforderungen, um mit dem jeweils nächsten Schritt der Installation fortzufahren. Wenn Sie eine Einstellung in einem vorherigen Schritt ändern möchten, klicken Sie auf 'Zurück'.
Sie können die Installation jederzeit abbrechen, indem Sie auf 'Beenden' klicken.
DRÜCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 87: Console Installation – Sprachauswahl, Einführung

Es folgt die OS und Plattform Erkennung, die Eingabeaufforderung des RCCMD Lizenzschlüssels und der Lizenzvertrag.

```
SysOS & Platform
----------------

OS & CPU architecture: unknown unknown GNU/Linux



DRÜCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:



================================================================================
Geben Sie ihren Lizenzschlüssel ein
-----------------------------------

Geben Sie ihren Lizenzschlüssel ein
Normalerweise ist der Lizenzschlüssel im Handbuch oder auf der CD-Hülle
vermerkt.
Lizenzschlüssel eingeben: 12SHARX3-1234567



================================================================================
Lizenzvertrag
-------------

Für die Installation und die Verwendung von RCCMD-Client müssen Sie den
folgenden Lizenzvertrag akzeptieren:


Copyright

The information contained in the manual of this product is nonconditional
and may be changed without due notice. GENEREX nor the reseller of this
product undertakes no obligations with this information. The software
described in this brochure is given on the basis of a license contract
and an obligation to secrecy (i.e. an obligation not to further publicise
the software material). The purchaser may make a single copy of the software
```

Abb. 88: Console Installation – OS/Plattform Erkennung, Lizenzeingabe, Lizenzvertrag

Wählen Sie die Produktfunktionen aus, die Sie installieren möchten, oder drücken Sie die „Enter“ Taste, wenn Sie alle Features installieren möchten.

```
================================================================================
Produktfunktionen auswählen
---------------------------

GEBEN SIE EINE DURCH KOMMAS GETRENNTE LISTE VON NUMMERN EIN, DIE FÜR DIE
FUNKTIONEN STEHEN, DIE SIE AUSWÄHLEN BZW. DEREN AUSWAHL SIE AUFHEBEN MÖCHTEN.
UM DIE BESCHREIBUNG EINER FUNKTION ANZUZEIGEN, GEBEN SIE '?<NUMMER>' EIN.  UM
DIE BESCHREIBUNG EINER FUNKTION ANZUZEIGEN, GEBEN SIE '?<NUMMER>' EIN. DRÜCKEN
SIE DIE EINGABETASTE, WENN SIE FERTIG SIND.

    1- [X] RCCMD
    2- [X] WebIf
    3- [X] XMessage

Wählen Sie die Funktionen aus, die vom Installer installiert werden sollen.
   :



================================================================================
Übersicht vor Installation
--------------------------

DRÜCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN.  FALLS DIE ANGABEN NICHT KORREKT
SIND, KLICKEN SIE AUF "Zurück", UM ÄNDERUNGEN VORZUNEHMEN.

Produktname:
    RCCMD

Installationsordner:
    /usr/rccmd

Produktkomponenten:
    RCCMD,
    WebIf,
    XMessage
```

Abb. 89: Console Installation – Produktfunktions-Auswahl, Übersicht

Soll RCCMD bei Systemstart automatisch ausgeführt werden?

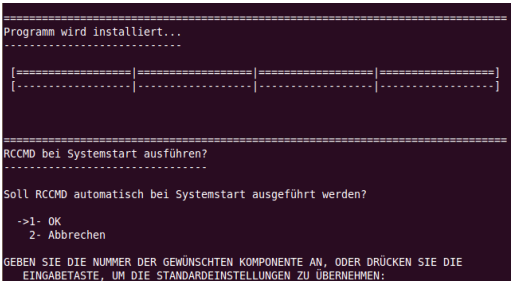
Programm wird installiert...
RCCMD bei Systemstart ausführen?
Soll RCCMD automatisch bei Systemstart ausgeführt werden?
->1- OK
2- Abbrechen
GEBEN SIE DIE NUMMER DER GEWÜNSCHTEN KOMPONENTE AN, ODER DRÜCKEN SIE DIE
EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ÜBERNEHMEN:

Abb. 90: Console Installation – Autostart

Es folgt die Protokoll und Port Auswahl für das Web-Interface.

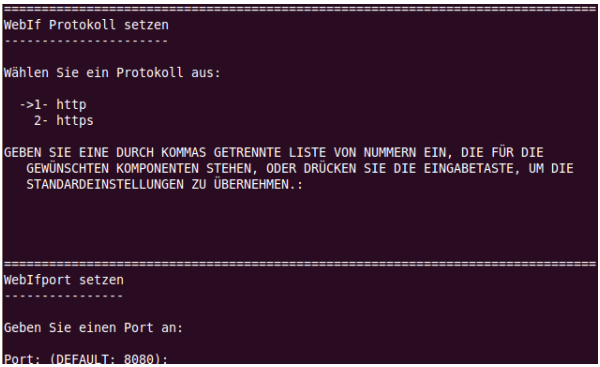
WebIf Protokoll setzen
Wählen Sie ein Protokoll aus:
->1- http
2- https
GEBEN SIE EINE DURCH KOMMAS GETRENNTE LISTE VON NUMMERN EIN, DIE FÜR DIE
GEWÜNSCHTEN KOMPONENTEN STEHEN, ODER DRÜCKEN SIE DIE EINGABETASTE, UM DIE
STANDARDEINSTELLUNGEN ZU ÜBERNEHMEN.:
WebIfport setzen
Geben Sie einen Port an:
Port: (DEFAULT: 8080):

Abb. 91: Console Installation – WebIf Auswahl

Es folgt ein Hinweis, dass eine RCCMD Konfiguration und Firewall Ausnahme erforderlich sind.

RCCMD-Konfiguration erforderlich
Eine Konfiguration des RCCMD ist erforderlich. Dazu kann das Webinterface unter
"http://<Adresse dieses Computers>:8080" genutzt werden.
Sollten Sie entscheiden den RCCMD mit der Standardkonfiguration zu starten, ist
es von jeder Netzwerkadresse aus möglich an diesen Nachrichten zu senden.
Bitte richten Sie eine oder mehrere IP-Adressen ein, die berechtigt sein sollen
diesem RCCMD Nachrichten zu senden.
DRÜCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:
Firewall Ausnahmen
Notwendige Firewall Ausnahmen.
Stellen Sie sicher, dass folgende Ports von keiner Firewall blockiert werden:
Ports 8080 TCP (WebIf Server), falls installiert
Ports 6003 & 5769 TCP,UDP (RCCMD)
DRÜCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 92: Console Installation – Hinweis, Firewall Ausnahme

Soll RCCMD jetzt gestartet werden? Somit ist RCCMD erfolgreich via Console installiert worden.

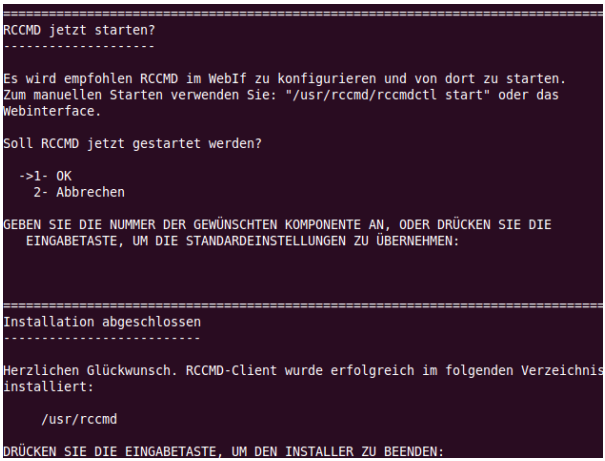
RCCMD jetzt starten?
Es wird empfohlen RCCMD im WebIf zu konfigurieren und von dort zu starten.
Zum manuellen Starten verwenden Sie: "/usr/rccmd/rccmdctl start" oder das
Webinterface.
Soll RCCMD jetzt gestartet werden?
->1- OK
2- Abbrechen
GEBEN SIE DIE NUMMER DER GEWÜNSCHTEN KOMPONENTE AN, ODER DRÜCKEN SIE DIE
EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ÜBERNEHMEN:
Installation abgeschlossen
Herzlichen Glückwunsch. RCCMD-Client wurde erfolgreich im folgenden Verzeichnis
installiert:
/usr/rccmd
DRÜCKEN SIE DIE EINGABETASTE, UM DEN INSTALLER ZU BEENDEN:

Abb. 93: Console Installation – RCCMD Start, Installations-Abschluss

3.4 RCCMD WebInterface (ab Version 4.2.0.0)

Ab der RCCMD Version 4.2.0.0 verfügt RCCMD über ein eigenes Webinterface, das die webbasierte Konfiguration bzw. Steuerung aus der Ferne ermöglicht. Nach der erfolgreichen Installation, wie in Kapitel 5 beschrieben, öffnet sich automatisch der Standardwebbrowser Ihres Betriebssystems.

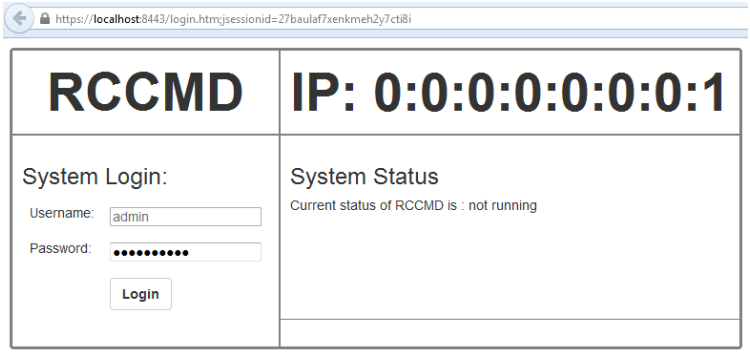

Abb. 94: RCCMD WebInterface

Im Menü „**Connections**“ können Sie die IP-Adressen der berechtigten RCCMD Sender (CS121/UPSMAN) eintragen. Klicken Sie auf „Insert“, um die IP-Adresse des ersten Senders einzutragen. Klicken Sie auf „Remove“, wenn Sie die eingetragene IP-Adresse herausnehmen möchten. Klicken Sie auf „Edit“, wenn Sie die eingetragene IP-Adresse bearbeiten möchten.

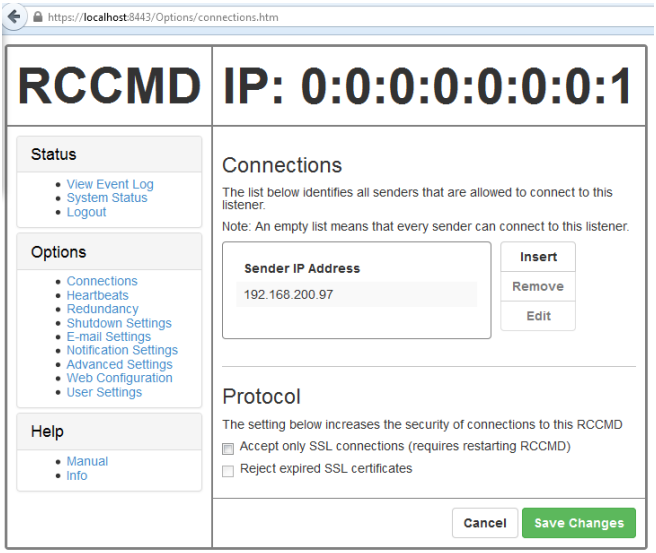

Abb. 95: RCCMD WebInterface – Connections

Achtung: **Wenn Sie hier keine Adresse eintragen, ist jeder Server in der Lage, einen Shutdown an diesen Client zu senden.**

Unter „**Protocols**“ kann definiert werden, ob RCCMD mit SSL Zertifikaten verwendet wird. Aktivieren Sie „Reject expired SSL certificates“, wenn Sie Verbindungen mit abgelaufenen SSL Zertifikaten ablehnen wollen. Weitere Informationen für RCCMD mit SSL finden Sie in Kapitel 6.6.1.

Klicken Sie vor Verlassen des „Connections“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Heartbeats**“ kann die Funktion „UPSMAN Alive Check“ aktiviert werden.

Dieser Check ist ein Signal, das an den CS121 oder UPSMAN via Port 5769 gesendet wird, um zu prüfen, ob der UPSMAN noch USV Daten hat. Wenn nicht, wird das Script File “Alive.Bat” ausgeführt, das eine entsprechende Nachricht als Pop-Up bringt.

Die Funktion “by the use CS121/UPSMAN Traps” ermöglicht UPSMAN/RCCMD/UNMS Meldungen, die den USV Status als Nachricht anzeigen. Wenn aktiviert, wird diese Funktion eine lokale Nachricht bringen, wenn der USV Status des UPSMAN/RCCMD Servers sich verändert.

Die Funktion „by polling CS121/UPSMAN every x seconds“ ermöglicht die reine Signalabfrage, ohne das Empfangen von USV-Werten bzw. Nachrichten.

Die Polling Rate (Standard 1800 Sekunden) definiert den Interval der UPSMAN Abfrage, connection retries (Verbindungswiederholungen, Standard 100) bedeutet, das nach 100 erfolglosen Verbindungsversuchen ein Alarm ausgelöst wird.

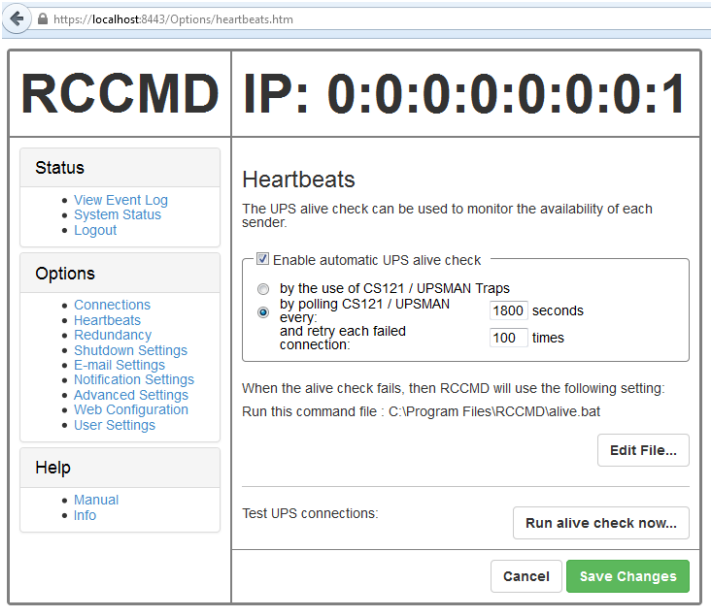

Abb. 96: RCCMD WebInterface – Heartbeats

Wenn Sie auf “Run alive check now…” klicken, wird das UPSMAN Alive Checking von der eingetragenen IP-Adresse gestartet (der Port 5769 wird getestet).

Klicken Sie vor Verlassen des „Heartbeats“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Redundancy**“ kann die Redundanz Management Funktion aktiviert werden. Der Redundanz Level definiert die Anzahl der redundanten Sender in der Redundanz Gruppe. Das bedeutet, dass bei einem Redunz Level von 1 beide RCCCMD Sender (CS121/UPSMAN) einen Shutdown gesendet haben müssen, bevor RCCMD seine Shutdown Sequenz startet.

Wenn RCCMD einen Shutdown unterdrückt, erhalten Sie eine Nachrichten Box aus der „Suppressed.bat“, die Sie verändern können, wenn Sie auf „Edit File...“ klicken.

Bitte beachten Sie, dass für das Zurücksetzen des Redundanz Alarms eine Event Konfiguration auf dem Sender (CS121/UPSMAN) erforderlich ist. Die Funktion „Send RCCMD cancle shutdown“ kann verwendet werden, um automatisch einen vorher abgesendeten Shutdown zu verwerfen. Wenn ein Shutdown unterdrückt wurde, wegen der zu diesem Zeitpunkt noch vorhandenen Redundanz, das Problem aber zwischenzeitlich an der USV gelöst wurde, kann mittels einem „Send RCCMD cancel

shutdown“ der Alarm zurückgesetzt werden. Durch diesen Befehl wird der RCCMD Client, der vorher das Shutdownsignal erhalten hat, aufgefordert, dieses wieder rückgängig zu machen.

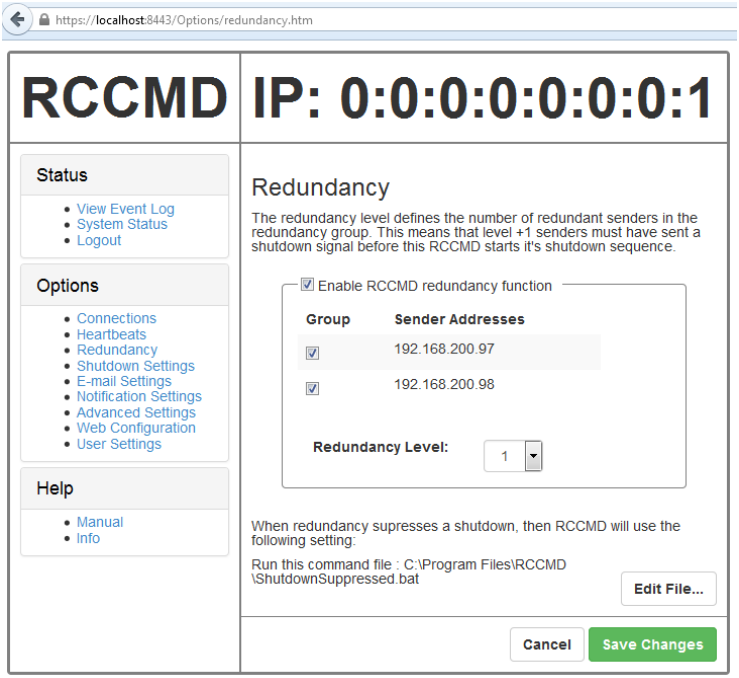

Abb. 97: RCCMD WebInterface – Redundancy

Schauen Sie bitte in das Kapitel 6.1 für ausführlichere Informationen zu RCCMD mit Redundanz.

Klicken Sie vor Verlassen des „Redundancy“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Shutdown Settings**“ können Sie die Shutdown Sequenz verändern bzw. erweitern. Als Standard wird die rccmd_shutdown.sh verwendet:

#!/bin/sh

This script is created by RCCMD shutdown sequence configuration.

This script is called by rccmd after receiving

the "SHUTDOWN" command from the network.

available command are:

shutdown -h now &

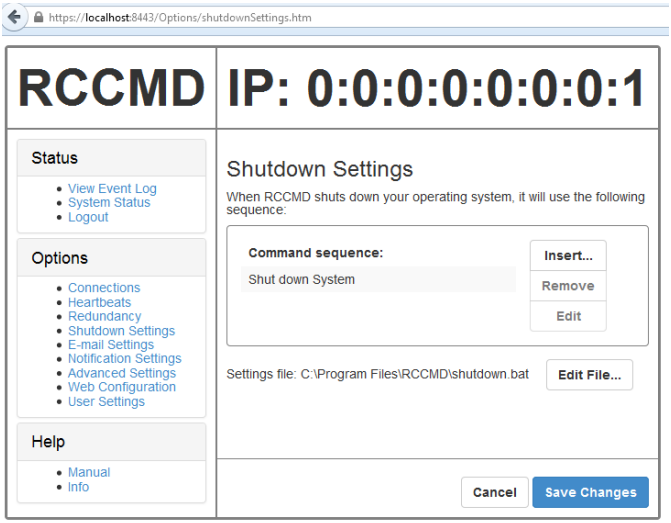

Abb. 98: RCCMD WebInterface – Shutdown Settings

Im Menü „**Notification Settings**“ können Sie die entsprechenden Standard Bat-Files für E-Mail, Message (Nachrichten) und Execute (auszuführende Kommandos) verändern bzw. erweitern, wenn Sie auf „Edit File...“ klicken.

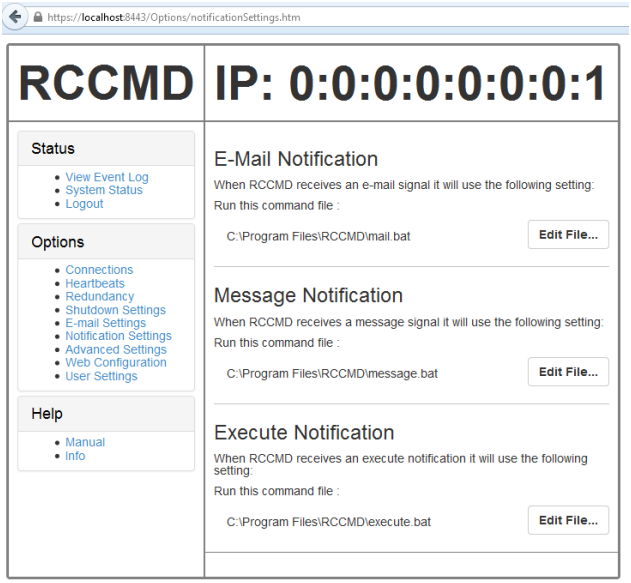

Abb. 99: RCCMD WebInterface – Notification Settings

Klicken Sie vor Verlassen des „Notification Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Advanced Settings**“ können Sie die maximale Grösse des Event Logfiles definieren, bei der das Überschreiben älterer Einträge beginnt, die RCCMD Bindings für die IP-Adresse und den RCCMD Listener TCP Port.

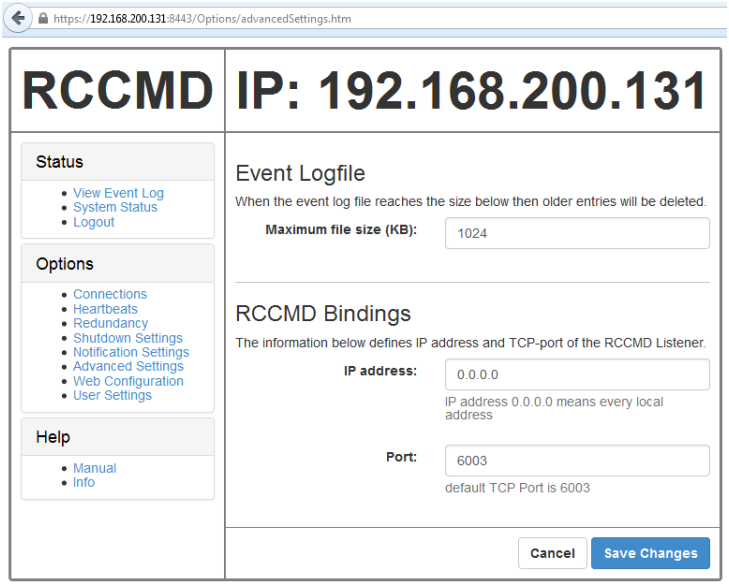

Abb. 100: RCCMD WebInterface – Advanced Settings

Klicken Sie vor Verlassen des „Advanced Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Web Configuration**“ besteht die Möglichkeit, das HTTPS Protokoll zu deaktivieren, um nur mit dem HTTP Protokoll zu arbeiten. Ab der RCCMD Version 4.2.3.0 gibt es die Möglichkeit, die Standard Ports für HTTP bzw. HTTPS zu ändern und den RCCMD WebIf neuzustarten.

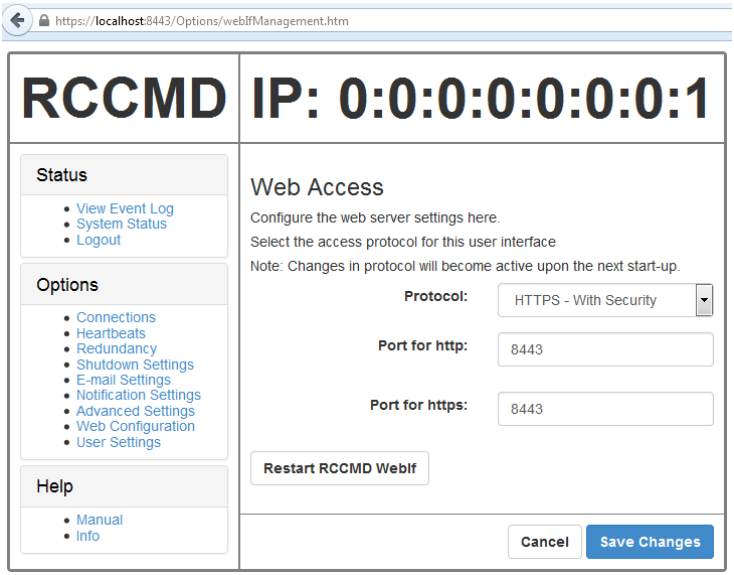

Abb. 101: RCCMD WebInterface – Web Access

Klicken Sie vor Verlassen des „Web Configuration“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**User Settings**“ können Sie das Standard Passwort für den Benutzer „admin“ wie gewünscht ändern und den RCCMD WebIf neustarten.

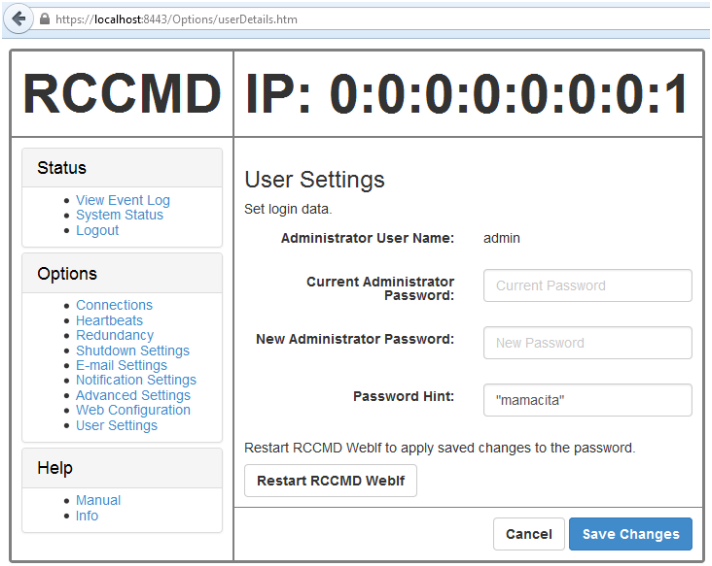

Abb. 102: RCCMD WebInterface – User Settings

Im Menü „**Status, View Event Log**“ können Sie die Protokollierung der bisherigen Ereignisse einsehen.

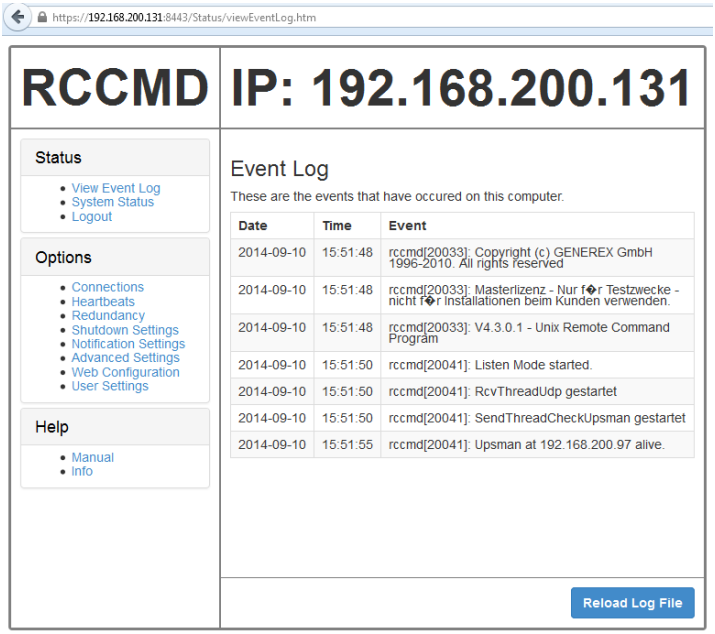

Abb. 103: RCCMD WebInterface – Event Log

Im Menü „**Status, System Status**“ können Sie den aktuellen Status von RCCMD überprüfen, den Status updaten und den RCCMD Dienst neustarten bzw. stoppen und starten.

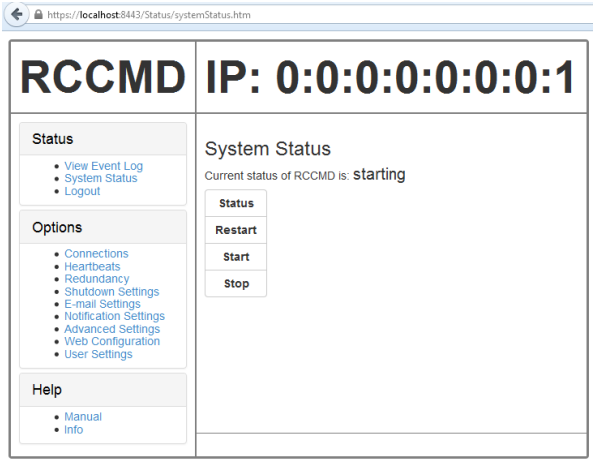

Abb. 104: RCCMD WebInterface – System Status

Im Menü „**Help**“ können Sie das RCCMD Benutzerhandbuch zu Ihrer Unterstützung aufrufen, können dem Link auf www.generex.de folgen und via „Info“ die Installer Version aufrufen.

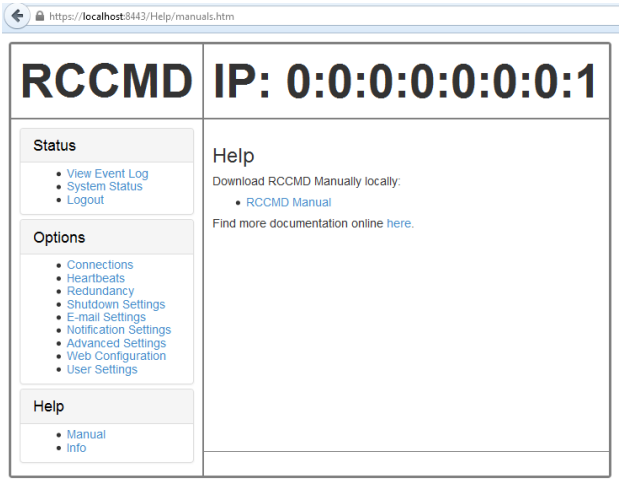

Abb. 105: RCCMD WebInterface – Help

3.5 RCCMD WebInterface Remote Zugriff

Ab der RCCMD Version 4.2.0.0 verfügt RCCMD über ein eigenes Webinterface, dass den Remote Zugriff ermöglicht. Bitte beachten Sie, dass der Firewall Port 8443 TCP freigeschaltet sein muss. Geben Sie in einem Webbrowser Folgendes ein, um sich remote auf den Rechner zu verbinden, auf dem RCCMD installiert wurde

https://IP-Adresse des RCCMD Rechners:8443

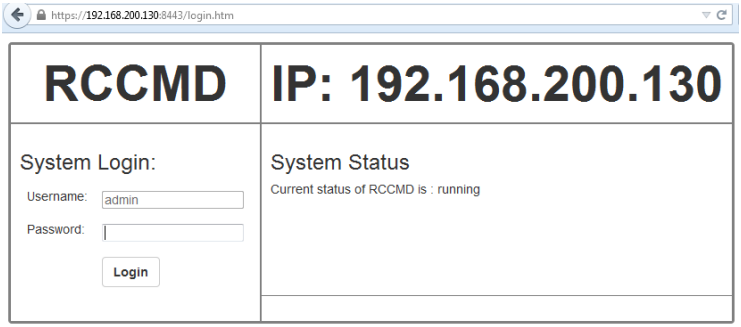

Abb. 106: RCCMD WebInterface – Remote Zugriff

Nun besteht die Möglichkeit, die Konfiguration bzw. Steuerung aus der Ferne auszuführen.

3.6 Automatisches Zurücksetzen des Redundanz Alarms

„Send RCCMD cancle shutdown“ kann verwendet werden, um automatisch einen vorher abgesendeten Shutdown zu verwerfen. Wenn ein Shutdown unterdrückt wurde, wegen der zu diesem Zeitpunkt noch vorhandenen Redundanz, das Problem aber zwischenzeitlich an der USV gelöst wurde, kann mittels einem „Send RCCMD cancel shutdown“ der Alarm zurückgesetzt werden. Durch diesen Befehl wird der RCCMD Client, der vorher das Shutdownsignal erhalten hat, aufgefordert, dieses wieder rückgängig zu machen.

Dieses Kommando kann indivduell in jedem Event/Alarm ihrer CS121 oder BACS WEBMANAGER Konfiguration eingefügt werden, macht allerdings nur dann Sinn, wenn der Event, der diesen Befehl absendet, auch tatsächlich dann aktiv ist, wenn die USV wieder als OK angesehen werden kann. Dafür geeignet sind Beispielsweise die Events „POWER RESTORED“, “BATTERY LOW OFF”, “UPSMAN STARTED” und “GENERAL ALARM OFF”, wenn diese in ihrem CS121 für diesen USV Typ angeboten werden. In diese „Entwarnungs-Ereignnisse“ würde dann der Job „Send RCCMD cancle shutdown“ eingetragen werden, sodass z. B. beim Neustart der USV, der Event „UPSMAN STARTED“ automatisch den betreffenden RCCMD Client wieder auf „normal“ zurücksetzt.

Alternativ: Sollte der Job „Send RCCMD cancle shutdown“ in ihrem CS121, UPSMAN oder BACS WEBMANAGER nicht vorhanden sein, kann alternativ auch der Job „Send RCCMD Command to remote client“ oder „Send RCCMD execute to remote client“ verwendet werden.

Der Parameter „WAKEUP“ hat die gleiche Funktion wie „Send RCCMD cancle shutdown“ und setzt den Redundanz Level eines RCCMD Clients in den Ausgangszustand zurück. Auch hier eignen sich die Events/Alarme POWER RESTORED, BATTERY LOW OFF, UPSMAN STARTED und GENERAL ALARM OFF besonders, um die Funktion „Send RCCMD Command to remote client“ mit dem „WAKEUP“ Befehl zu konfigurieren.

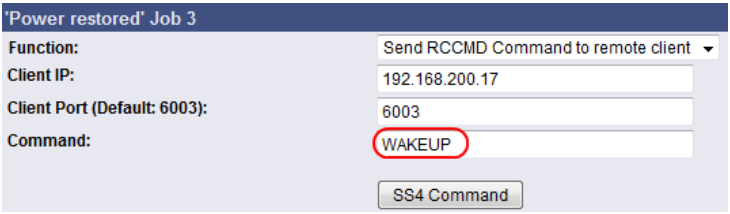

Abb. 107: CS121 Konfiguration „WAKEUP“ Befehl

Klicken Sie im CS121 Menü „Events/Alarms“ auf „Power restored“, und fügen Sie einen neuen Job hinzu. Wählen Sie die Funktion „Send RCCMD Command to remote client“ aus, tragen Sie die entsprechende IP-Adresse des Clients ein, und schreiben Sie den Befehl „WAKEUP“ in die „Command“ Zeile.

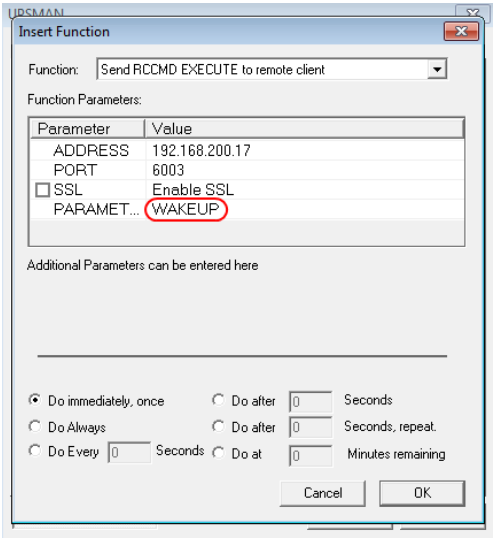

Abb. 108: UPSMAN Konfiguration „WAKEUP“ Befehl

Öffnen Sie die UPSMAN Konfiguration, und klicken Sie auf „Avanced Users“, „Events“, „Power restored“ und „Insert“. Fügen Sie die Funktion „Send RCCMD EXECUTE to remote client“ hinzu, und tragen Sie die entsprechende IP-Adresse des Clients ein, und schreiben Sie den Befehl „WAKEUP“ in die Parameter Zeile.

```
01/05/2010,14:59:54, RCCMD: RcvThreadUdp started
01/05/2010,14:59:54, RCCMD: RCCMD Listen Mode started.
01/05/2010,14:59:54, RCCMD: SendThreadCheckUpsman started
01/05/2010,14:59:54, RCCMD: RCCMD Trap client logged on to 192.168.222.177
01/05/2010,14:59:54, RCCMD: RCCMD Trap client logged on to 192.168.222.246
01/05/2010,15:01:01, RCCMD: RCCMD Trying to start program/job: ".\message.bat" "UPSMAN Notification
01/05/2010,15:01:01, RCCMD: RCCMD program/job: ".\message.bat" "UPSMAN Notification [192.168.222.177]
01/05/2010,15:01:03, RCCMD: RCCMD message received from 192.168.222.177
01/05/2010,15:01:04, RCCMD: Shutdown suppressed, redundancy-level = 1, failure count = 1.

01/05/2010,15:01:04, RCCMD: RCCMD Trying to start program/job: C:\RCCMD\ShutdownSuppressed.bat
01/05/2010,15:01:04, RCCMD: RCCMD program/job: C:\RCCMD\ShutdownSuppressed.bat executed. OK
01/05/2010,15:02:06, RCCMD: RCCMD Trying to start program/job: ".\message.bat" "UPSMAN Notification
01/05/2010,15:02:06, RCCMD: RCCMD program/job: ".\message.bat" "UPSMAN Notification [192.168.222.177]
01/05/2010,15:02:09, RCCMD: RCCMD message received from 192.168.222.177
01/05/2010,15:02:09, RCCMD: WAKEUP command received from 192.168.222.177.

01/05/2010,15:02:09, RCCMD: WAKEUP IP 192.168.222.177
```

Abb. 109: „WAKEUP“ Befehl im RCCMD Log

3.7 RCCMD mit SSL auf UNIX

Das *Secure Sockets Layer* (SSL) Protokoll ist ein kryptografisches Protokoll, das Sicherheit und Datenintegrität für Kommunikationen in TCP/IP Netzwerken bietet.

Stellen Sie über einen Webbrowser eine Verbindung zum CS121 SNMP Adapter her. Klicken Sie im Konfigurations-Menü auf “Network & Security”, und setzen Sie den Haken bei “Use RCCMD SSL”.

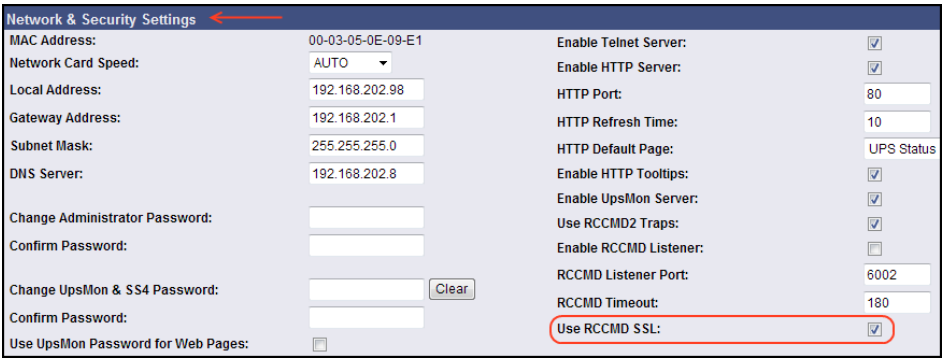

Abb. 110: RCCMD SSL Konfiguration

Das SSL Netzwerk Feature erfordert einen korrekten Zeitstempel. Konfigurieren Sie im „Timeserver“ Menü eine entsprechende IP-Adresse.

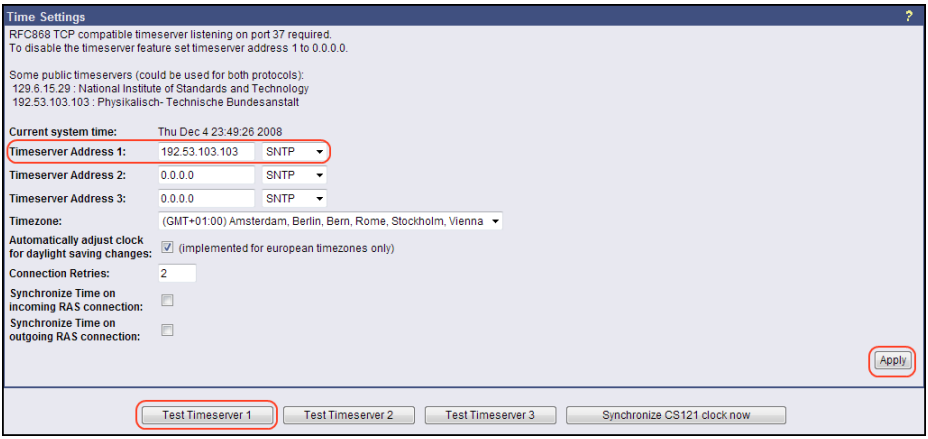

Abb. 111: Timeserver Konfiguration

Klicken Sie auf das „Save Configuration“ Menü, und bestätigen Sie Ihre Einstellungen mit „Save, Exit & Reboot“.

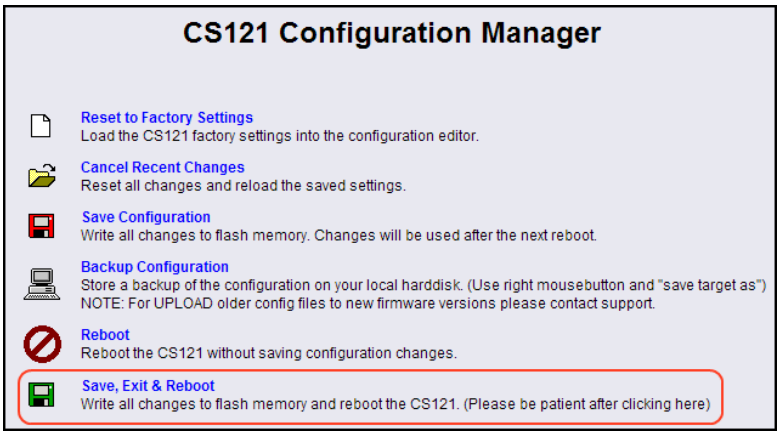
CS121 Configuration Manager
Reset to Factory Settings
Load the CS121 factory settings into the configuration editor.
Cancel Recent Changes
Reset all changes and reload the saved settings.
Save Configuration
Write all changes to flash memory. Changes will be used after the next reboot.
Backup Configuration
Store a backup of the configuration on your local harddisk. (Use right mousebutton and "save target as")
NOTE: For UPLOAD older config files to new firmware versions please contact support.
Reboot
Reboot the CS121 without saving configuration changes.
Save, Exit & Reboot
Write all changes to flash memory and reboot the CS121. (Please be patient after clicking here)

Abb. 112: Speichern der Einstellungen

Öffnen Sie den RCCMD Web Configurator, und aktivieren Sie das SSL Netzwerk Feature.

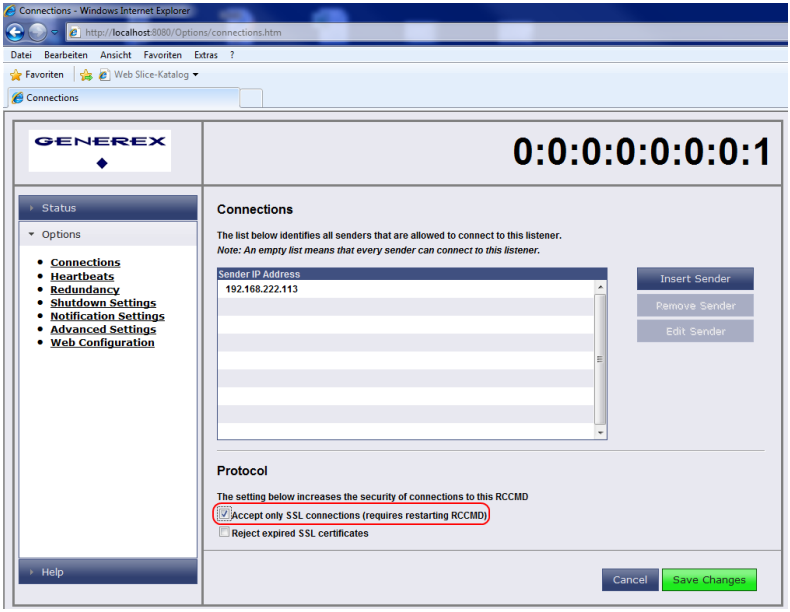

Abb. 113: SSL Konfiguration

Wenn Sie abgelaufene Zertifikate akzeptieren möchten, aktivieren Sie die Funktion “Reject expired SSL certificates”.

Starten Sie RCCMD via „Restart RCCMD“ Button im Menü System Status.

3.7.1 RCCMD mit eigenen SSL Zertifikaten

In diesem Abschnitt beschreiben wir, wie man ein eigenes SSL Zertifikat mit RCCMD nutzen kann, z. B. OpenSSL (http://www.openssl.org):

Sein Sie Ihre eigene Zertifizierungsstelle (CA)

Mit der Nutzung von OpenSSL ist es sehr einfach, sein eigener Zertifizierer zu werden. Nutzen Sie einfach diesen Befehl:

```
CA.pl -newca
```

Fertig! Vergewissern Sie sich, dass Sie einen gebräuchlichen CN (gewöhnlichen Namen) verwendet haben.

Erstellen des RCCMD Zertifikats

Nun müssen Sie Ihr Zertifikat für RCCMD erstellen. Da es für die Verifizierung den CN nutzt, sollte das Zertifikat diesen Namen auch enthalten, den Sie für das CA gewählt haben. Die private Schlüssel muss nicht verschlüsselt werden, um den RCCMD Client (Dienst) zu starten. Dafür nutzen wir die "-nodes" Option und den "-newreq" Befehl:

```
CA.pl -newreq -nodes
```

Signieren mit CA:

```
CA.pl -sign
```

Erstellen Sie nun eine leere Datei mit dem Namen "rccmd.pem", und kopieren Sie die Zertifizierungsinformationen von "newcert.pem" (RCCMD Zertifikat), "newkey.pem" (Privater Schlüssel) und "cacert.pem" (CA) in diese Datei. Bitte beachten Sie, dass das exakte Kopieren erforderlich ist, damit Sie es ohne Probleme nutzen können.

Nutzung des eigenen RCCMD Zertifikats

Führen Sie die folgenden Schritte auf jedem RCCMD Client und Sender aus, um die Konfiguration abzuschliessen.

- Stellen Sie ein Backup von der existierenden "rccmd.pem" her
- Ersetzen Sie die "rccmd.pem" mit Ihrer eigenen
- Starten Sie den RCCMD Client neu

Starten Sie den RCCMD Sender neu!

3.8 Alternative RCCMD Konfiguration über Editor

Die Konfiguration von RCCMD muss per Editor erfolgen, wenn Sie keine grafische Schnittstelle haben. Die Konfigurationsdatei ist „rccmd.cfg" und liegt im Standard RCCMD Verzeichnis (/usr/rccmd). Die Datei enthält im Kommentar die Beschreibung der einzelnen Konfigurationspunkte. Nachfolgend ein Beispielauszug aus der „rccmd.cfg". Ändern Sie die Eingaben entsprechend Ihrer Installation:

```
#######################################
# RCCMD Configuration
#######################################
# Bind on Interface
# Defines on which interface we listen for incoming commands
# Default: 0.0.0.0 (All possible interfaces on this host)
ListenAddress=0.0.0.0
# Listen on Port
# Defines on which interface port we listen for incoming commands.
# Default: 6003
ListenPort=6003
# Enable UDP
# Defines if we should listen for rccmd (UDP) broadcasts
# Default: true
ListenUDP=true
# Access Control List
# A list of valid sender addresses, only its members can connect to us.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (Everyone is allowed to connect to us)
AllowedAddresses=
# Alive Check
# Enable Alive Check
# Defines if we should perform UPSMan alive checking.
# Default: false
AliveEnabled=false
# Alive Check Rate
# Defines the interval of UPSMan alive checking, in seconds.
# Default: 1800
AliveInterval=1800
```

Alive Retry Rate

Defines the number of UPSMan alive checking retries, in case of problems.

Default: 0

AliveRetries=5

Alive Check Group Members List

A list of UPS device addresses that should be checked periodically.

Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".

Default: <empty> (No alive checking)

AliveAddresses=

Alive Program

Full path to script that is executed when an alive check fails.

Default: rccmd_notalive.sh

AliveProg=

Redundancy Mode

Enable Redundancy

Defines if we should operate in redundancy mode.

Requires an enabled <Alive Check> configuration.

Default: false

RedundancyEnabled=false

Redundancy Group Members List

A list of redundancy group member addresses, must be also in <AliveAddresses>.

Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".

Default: <empty> (No redundancy available)

RedundancyAddresses=

Redundancy Level

Defines how many of the <RedundancyAddresses> are redundant.

Shutdown is executed when the number of shutdown requests exceeds this number.

Default: 0 (No redundancy available)

RedundancyLevel=0

Enable Redundancy Script

Defines if we should NOT execute a script when redundancy suppresses a shutdown.

Default: false.

RedundancyBatchSuppress=false

Redundancy Script

Full path to script that is executed when redundancy suppresses a shutdown.

Default: ShutdownSuppressed.sh

RedundancyBatchFile=

Wenn Sie keine Einträge in der Standard „rccmd.cfg“ Datei verändern, werden alle eingehenen RCCMD Kommandos von jedem Sender ausgeführt und das Standard Shutdown-Skript „rccmd_shutdown.sh“ wird verwendet.

3.9 Alte RCCMD Konfiguration auf UNIX OS

Fügen Sie die IP-Adresse des RCCMD Servers hinzu, der authorisiert ist, ein Shutdown Signal zu diesem Client zu senden.

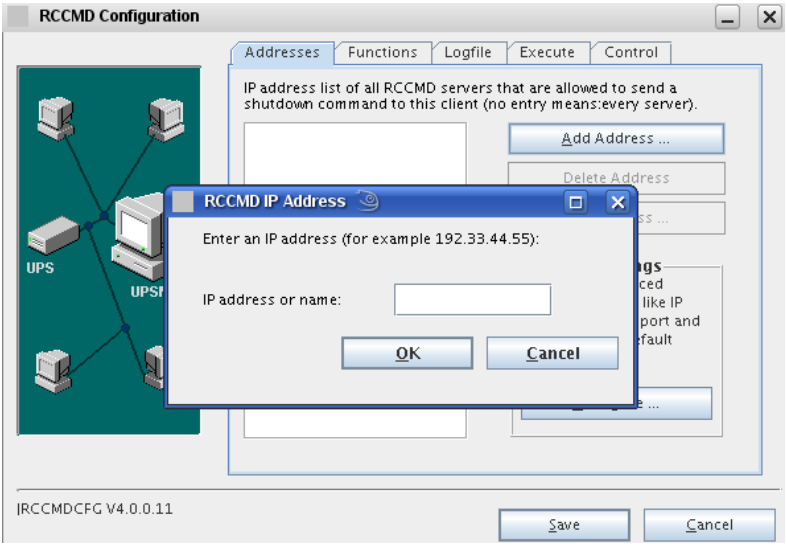

Abb. 114: Konfiguration – IP-Adressen Fenster

Achtung: **Wenn Sie keine Adresse eintragen, ist automatisch jeder Server authorisiert, ein Shutdown Signal zu senden. Wenn mehr als ein CS121 oder UPSMAN im Netzwerk existieren, also**

eine Redundanz Situation, müssen Sie mehrere Adressen als authorisierte Sender eintragen.

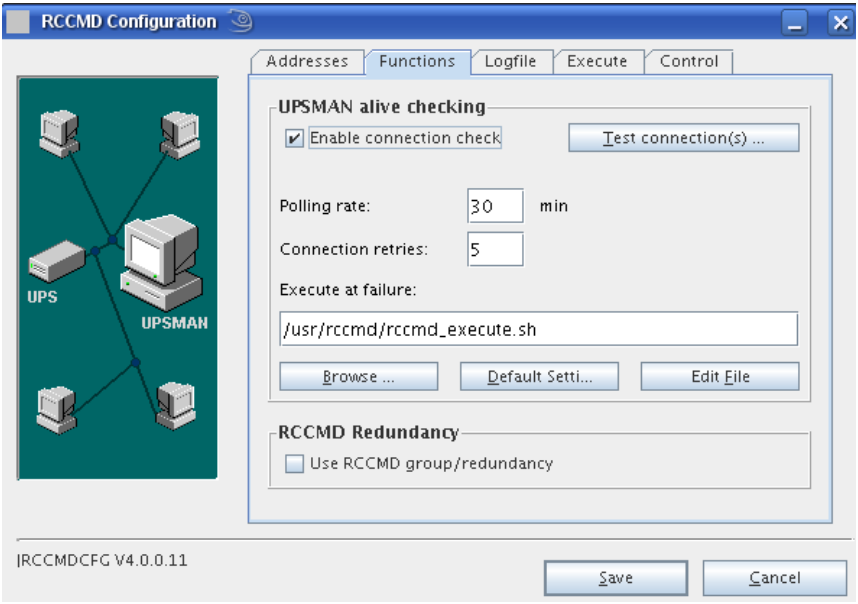

Abb. 115: Konfiguration – Functions

Wenn Sie die Funktion “UPSMAN Alive Checking” nutzen möchten (empfohlen), haken Sie die entsprechende Box an. Dieser Check ist ein Signal, dass an den CS121 oder UPSMAN via Port 5769 gesendet wird, um zu prüfen, ob der UPSMAN noch USV Daten hat. Wenn nicht, wird das Script File “rccmd_execute.sh” ausgeführt, das eine entsprechende Nachricht als Pop-Up bringt. Die *Polling Rate* (Standard 30 Minuten) definiert den Interval der UPSMAN Abfrage, *connect retries* (Verbindungswiederholungen, Standard 5) bedeutet, das nach 5 erfolglosen Verbindungsversuchen ein Alarm ausgelöst wird.

Die Funktion “Use RCCMD Traps” ermöglicht UPSMAN/RCCMD/UNMS Meldungen, die den USV Status als Nachricht anzeigt. Wenn aktiviert, wird diese Funktion eine lokale Nachricht bringen, wenn der USV Status des UPSMAN/RCCMD Servers sich verändert.

Wenn Sie auf “Test connections…” klicken, wird das UPSMAN Alive Checking von der eingetragenen IP-Adresse gestartet (der Port 5769 wird getestet).

Wenn Sie auf “Browse…” klicken, werden Sie eine Auswahl der Standard SH-Files erhalten.

Wenn Sie auf „Default Setting“ klicken, werden Sie zurück zum „rccmd_execute.sh“ File gelangen.

Bei einem Fehler von dem UPSMAN Alive Check können Sie eine auszuführende Datei konfigurieren oder das Standard File editieren.

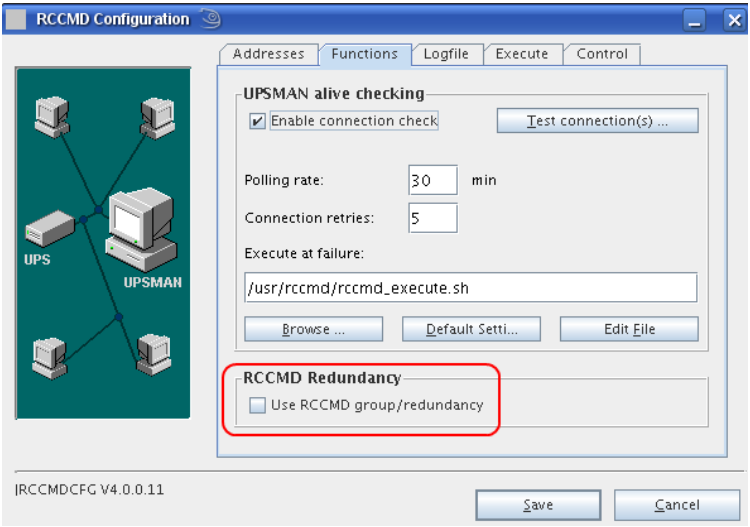

Abb. 116: Konfiguration – RCCMD Redundanz

Bei der USV Installation bietet RCCMD eine Redundanz Management Funktion wie folgt an:

Jede USV muss mit einem CS121 oder einem UPSMAN Software Computer ausgestattet sein. Wenn Sie die Box “Use RCCMD group/redundancy” anhaken, gelangen Sie zu einem Menü, welcher CS121/UPSMAN diesen RCCMD Client versorgt. Z.B.: Wenn 4 CS121/UPSMAN in 4 USVen installiert sind, dann kann jeder ein Shutdown Signal zu diesem RCCMD Client absetzen.

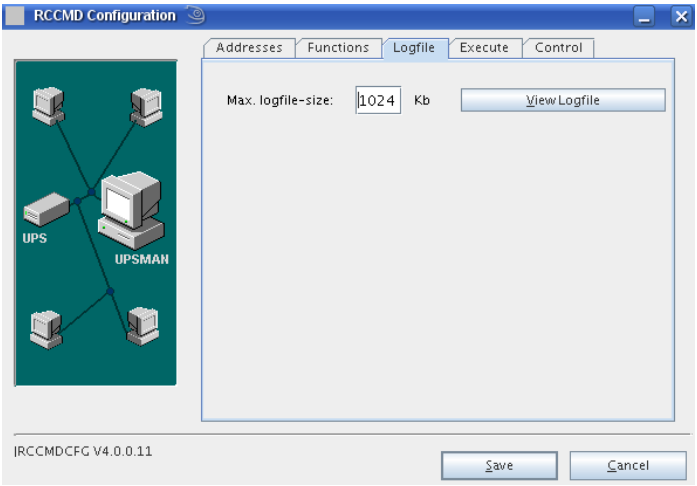

Abb. 117: Konfiguration – RCCMD Log File

Sie können die Log File Grösse konfigurieren und die auszuführenden Files editieren.

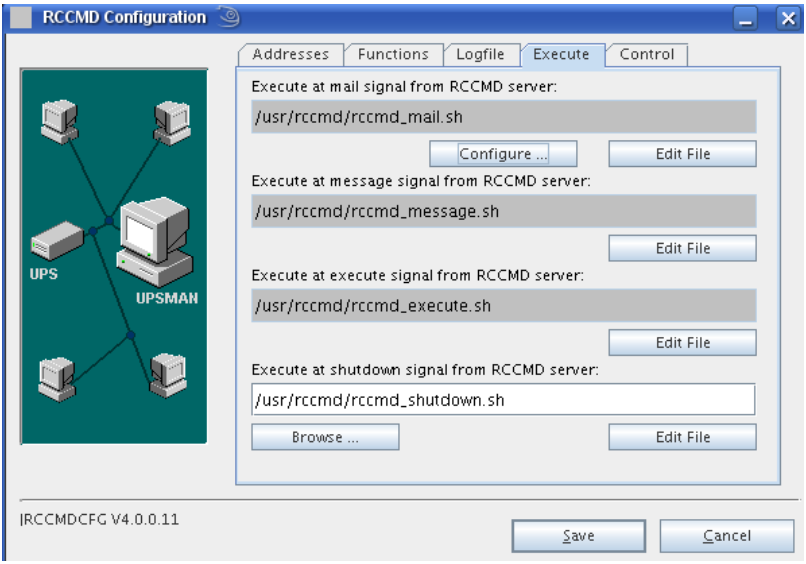

Abb. 118: Konfiguration – RCCMD Execute

Wenn Sie auf “Configure…” klicken, können Sie die Email Einstellungen vornehmen und die Mailfunktion von RCCMD nutzen.

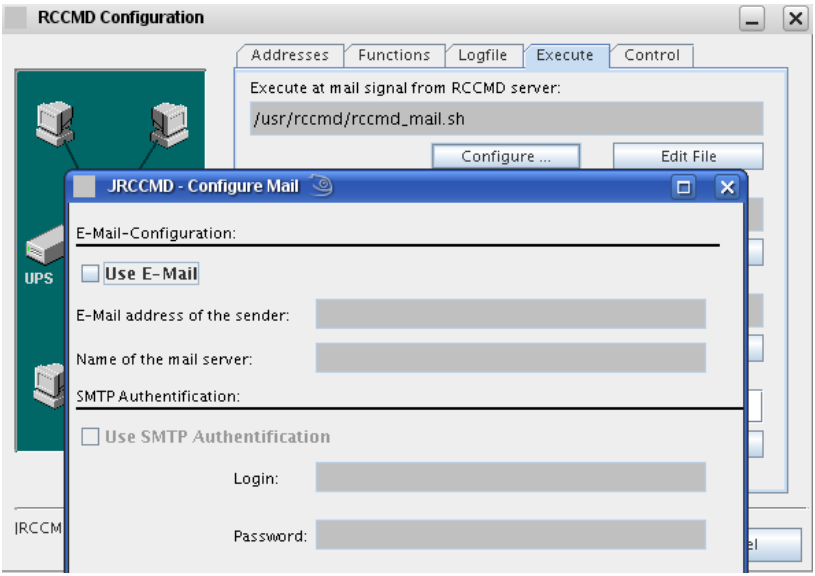

Abb. 119: Konfiguration – RCCMD Configure Email

Ab der RCCMD Version 4.0.2.0 gibt es auch eine grafische Konfiguration der Shutdown Sequenz.

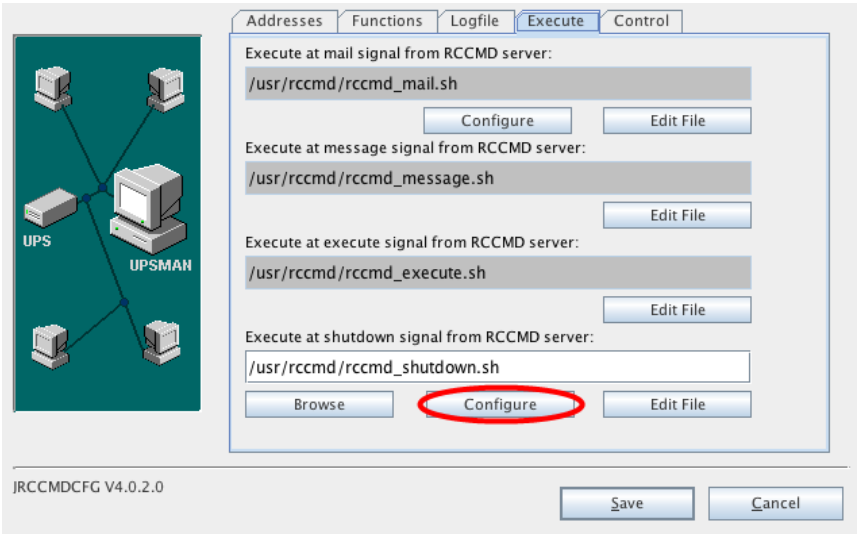

Abb. 120: Konfiguration – RCCMD Shutdown.sh

Klicken Sie auf „Configure“, um die Shutdown Sequenz zu öffnen.

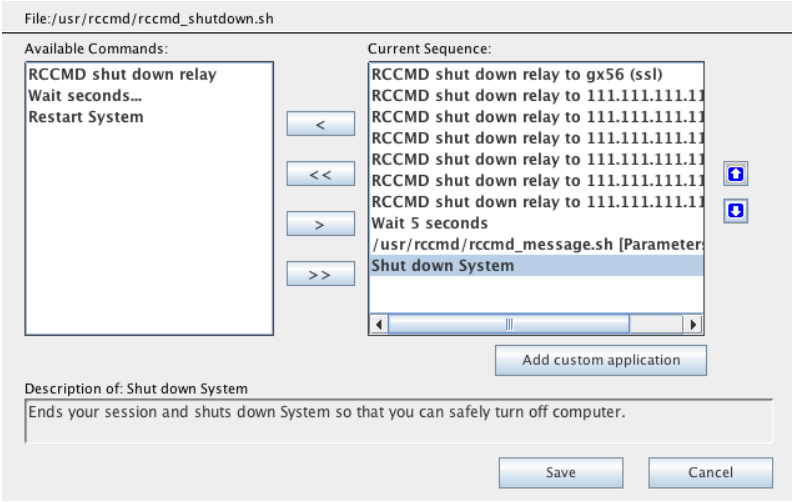

Abb. 121: Konfiguration – RCCMD Shutdown Sequenz

Die folgenden Befehle sind für die Shutdown Sequenz Konfiguration erhältlich:

RCCMD shutdown relay: Leitet einen RCCMD Shutdown Befehl an eine andere Workstation weiter (siehe auch Kapitel 5.4, Seite 75).

Wait seconds...: Warten eines Zeitraums in Sekunden, bis das nächste Kommando ausgeführt wird.

Restart System: Beendet Ihre Sitzung, fährt das System herunter und startet es neu.

Shutdown System: Beendet Ihre Sitzung und fährt das System herunter, sodass Sie sicher die Stromzufuhr unterbrechen können.

Über den „Control“ Button gelangen Sie zu der folgenden Maske:

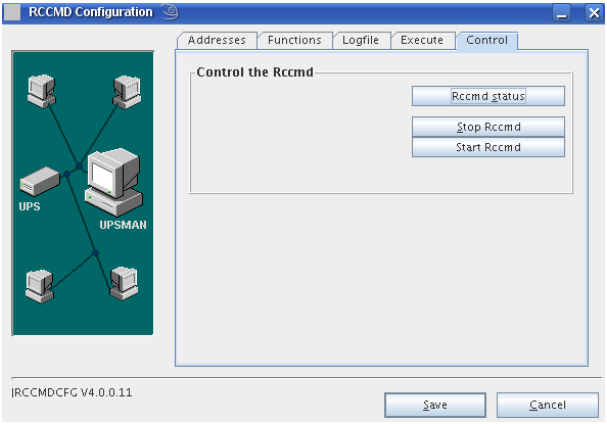

Abb. 122: Konfiguration – RCCMD Control

3.9.1 Der RCCMD Client als Relay Station

Wenn Sie eine grössere Anzahl von RCCMD Empfänger erreichen möchten, muss der CS121 Adapter als Relay Station fungieren. Der Empfänger wird so konfiguriert, dass er beim Erhalten eines RCCMD Signals eine Script startet, das weitere RCCMD Signale versendet. Diese Workstation ist dann Empfänger und Sender zur gleichen Zeit und somit eine wichtige Verbindung in der USV Überwachungskette. Der Gebrauch von einem RCCMD Client als Relay Station macht die Überwachung von mehreren hundert RCCMD Clients sehr viel einfacher als die Konfiguration über das Web-Interface des CS121. Außerdem haben alle Webbrowser Event Konfigurationen eine Sicherheits-Limitierung, sodas es erforderlich ist, diese Relay Funktion zu nutzen, wenn die Anzahl der Jobs 50 pro Event auf dem CS121 HW131 übersteigt.

So richtet man ein RCCMD Relay (Weiterleitung des Shutdown-Signals) ein:

- Öffnen Sie die Datei „rccmd_shutdown.sh“ mit einem Editor.
- Fügen Sie vor dem Shutdown des Computers (in der Zeile „shutdown –h now“) die Relay Aufrufe ein, z.B. einen Aufruf des mitgelieferten Scriptes „send_shutdown.sh“.
- Diesem Script können gleich mehrere IP-Adressen oder DNS-Namen der gewünschten Relay Empfänger übergeben werden, z.B:

```
./send_shutdown.sh -a 10.10.10.10 -a 10.10.10.11 -a 10.10.10.12
```

- Speichern Sie die Änderungen der Datei „rccmd_shutdown.sh“.

Ab der RCCMD Version 4.0.2.0 gibt es auch eine grafische Konfiguration der Shutdown Sequenz.

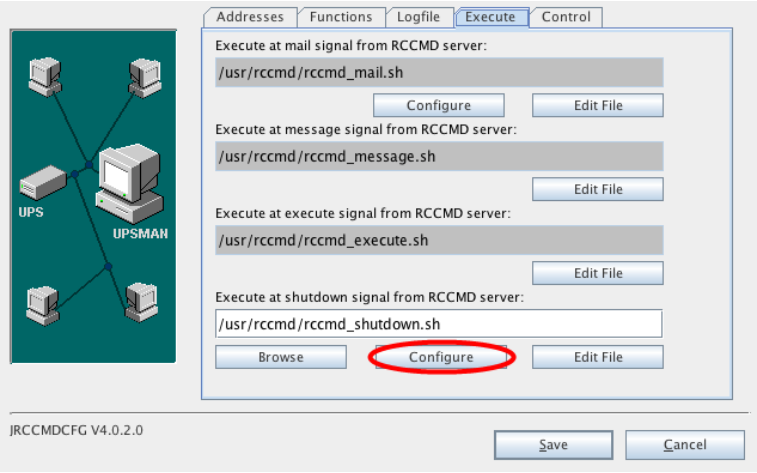

Abb. 123: Konfiguration – RCCMD Shutdown.sh

Klicken Sie auf „Configure“, um die Shutdown Sequenz zu öffnen.

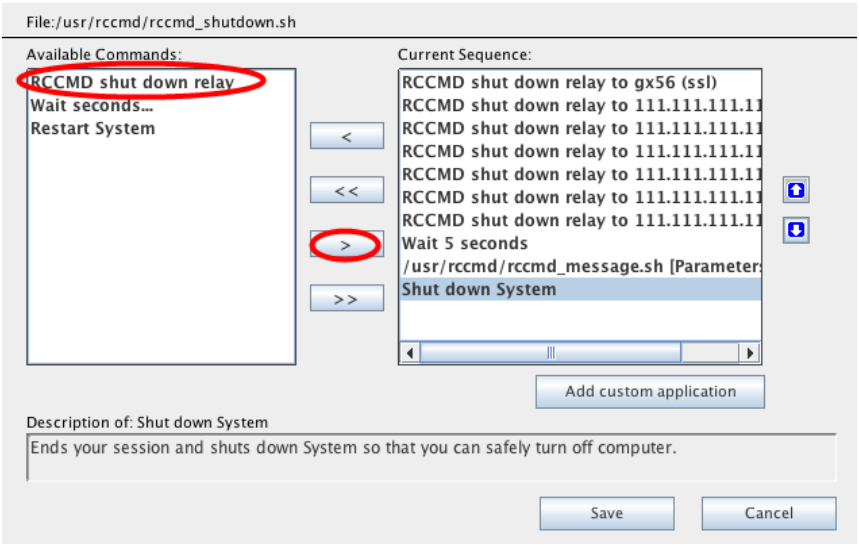

Abb. 124: Konfiguration – RCCMD Shutdown Sequenz

Wenn Sie „RCCMD shut down relay markiert haben und den Pfeil „>“ klicken, öffnet sich folgendes Fenster, in dem man den gewünschten IP-Adressen-Bereich eingeben kann oder eine einzelne IP-Adresse bzw. Hostnamen.

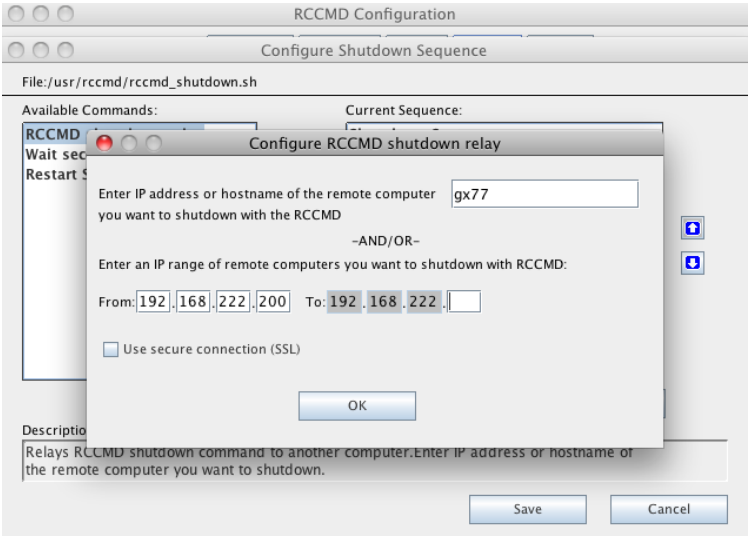
RCCMD Configuration
Configure Shutdown Sequence
File:/usr/rccmd/rccmd_shutdown.sh
Available Commands:
Current Sequence:
Configure RCCMD shutdown relay
Enter IP address or hostname of the remote computer you want to shutdown with the RCCMD
gx77
-AND/OR-
Enter an IP range of remote computers you want to shutdown with RCCMD:
From: 192 . 168 . 222 . 200
To: 192 . 168 . 222 .
Use secure connection (SSL)
OK
Relays RCCMD shutdown command to another computer.Enter IP address or hostname of the remote computer you want to shutdown.
Save
Cancel

Abb. 125: Konfiguration – RCCMD Relay Konfiguration IP-Adressen-Bereich

Ausserdem kann man hier auch die SSL-Funktion aktivieren (siehe auch Kapitel 5.5).

Um einzelne IP-Adressen aus dem Bereich zu entfernen, markieren Sie die Zeile auf der rechten Seite mit der entsprechenden IP-Adresse, und klicken Sie auf den Pfeil „<“.

3.10 UNIX RCCMD Konfiguration mit CURSES Library

Hinweis: **Dieses Kapitel gilt für den Lauscher-Modus.**

RCCMD V2 im Lauscher Modus sollte mit Hilfe eines Konfigurations File konfiguriert werden. Standardmässig sucht RCCMD ein File mit dem Namen rccmd.cfg in seinem Startverzeichnis (/usr/ups). Dieses File sollte mit rccmd_conf. generiert werden. Rccmd_conf. Ist ein kleines Cursor basiertes Tool, welches auf einer Konsole, einem Terminal oder einer Terminal-Emulation unter X Windows System (z.B.: xterm) läuft.

Note: **Die Inhalte von rccmd.cfg sind grundlegend für die System Security. Nur der Sytem User “Root” sollte über Schreibrechte verfügen. Das Tool „rccmd_conf“ wird von neueren Betriebssystemen nicht unterstützt. Wenn Sie versuchen, das Tool auf einem nicht unterstützten Betriebssystem auszuführen, erhalten Sie die Fehlermeldung über die nicht vorhandene „curses“ library.**

Run rccmd_conf:

$ su -

Password:

cd /usr/ups

./rccmd_conf

Wenn rccmd.cfg nicht existiert (z.B.: wenn Sie rccmd_conf das erste Mal starten), erscheint folgende Meldung:

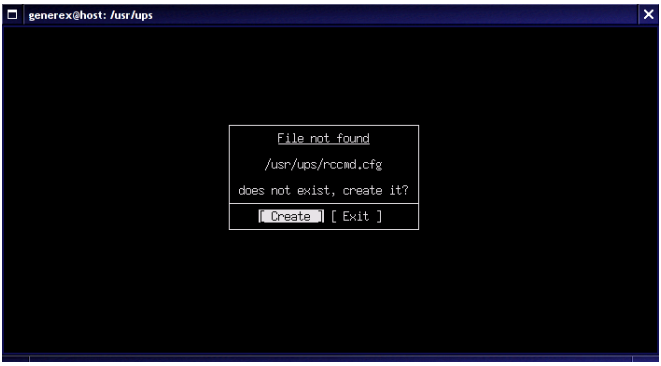

Abb. 126: Erstellung des Konfigurations-Files

Zum Fortfahren drücken Sie [Tab] solange [Create] markiert ist. Dann drücken Sie [Enter] oder wählen [Exit].

Wenn das File rccmd.cfg bereits existiert, wird rccmd_conf zu seinem Hauptkonfigurations-Menü wechseln.

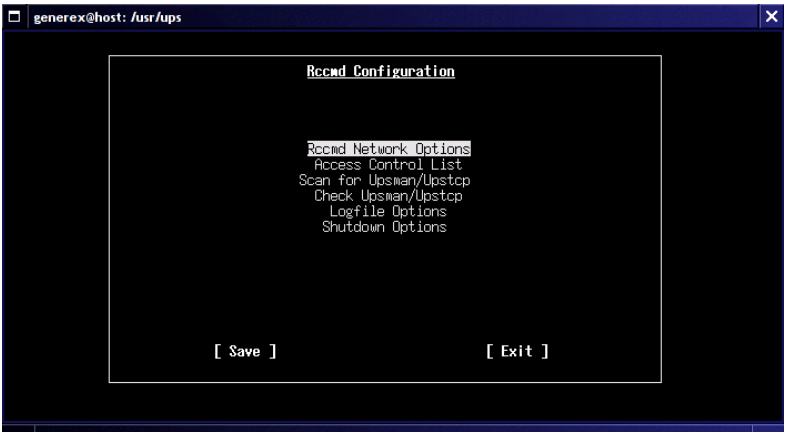

Abb. 127: RCCMD Konfigurations-Menü UNIX

Um zwischen den Menüeinträgen zu wechseln, drücken Sie [Tab] und/oder die Pfeiltasten. Um einen Eintrag auszuwählen, drücken Sie [Enter].

Es ist nicht erforderlich, von oben nach unten zu arbeiten. Sie können die Menüpunkte in beliebiger Reihenfolge konfigurieren. Wenn Sie nichts konfigurieren, werden die Standardwerte verwendet, wenn Sie auf [Save] drücken. Wir empfehlen, RCCMD (rccmd.cfg) individuell zu konfigurieren, um alle Features nutzen zu können und um die Sicherheit zu erhöhen.

Konfiguration der “RCCMD Network Options”

In diesem Fenster können Sie die Netzwerk relevanten Optionen von dem RCCMD Lauscher konfigurieren. Um zwischen den Options-Feldern zu wechseln, nutzen Sie die [Tab] Taste.

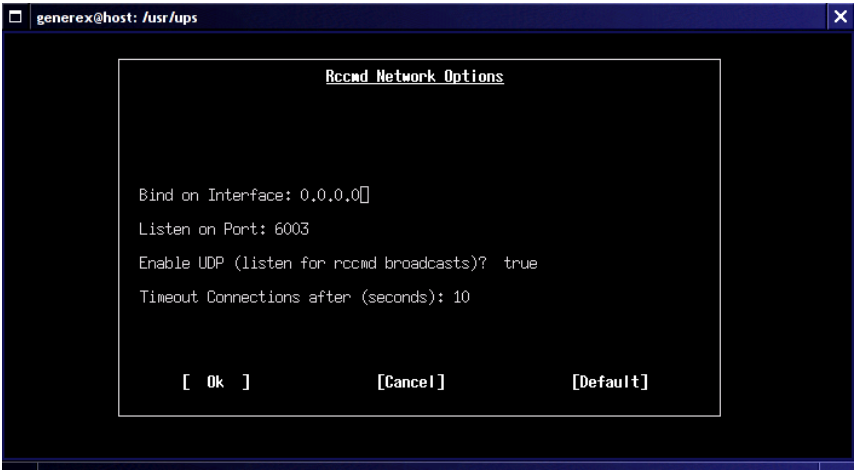

Abb. 128: RCCMD UNIX Netzwerk Optionen

Schnittstellenanbindung:

Mit dieser Option wird definiert, welche Netzwerk-Schnittstelle an das Haupt TCP Lauscher *Socket* angebunden ist. Sie können jede gültige IP-Adresse angeben, auf die der Host erreicht werden kann.

Der Standardwert für diese Option ist 0.0.0.0, dies ist ein gültiger Wert, der bedeutet, dass auf alle möglichen Schnittstellen gelauscht wird. Wenn der Host eine Dial-Up-Verbindung zum Internet hat, sollten Sie den Standardwert verändern, um sicherzustellen, das RCCMD nicht vom Internet aus verbunden wird. In diesem Fall sollten Sie die IP-Adresse von dem Host eintragen, auf dem der RCCMD Lauscher läuft.

Beispiel:

Ihr Computer läuft in einem privaten Netzwerk in dem 192.168.1.0/24 Adressbereich. Der RCCMD Lauscher läuft auf der vergebenen IP-Adresse192.168.1.9. Sie sollten diese Adresse im Feld “Bind On Interface” eintragen, um sicherzustellen, dass nur Workstations aus dem privaten Netzwerk eine Verbindung zu RCCMD herstellen können.

Lauschen auf Port:	Dies ist der Port, auf dem RCCMD als Lauscher läuft. Der erlaubte Wertebereich liegt zwischen 1 und 65535 (inklusive). Der Standard-Port ist 6003. Wenn Sie den Port von dem RCCMD Lauscher verändern, müssen Sie auch den Port von dem RCCMD Sender verändern, um eine Verbindung herzustellen. Es ist eigentlich nicht notwendig, den Standard-Port zu verändern.
UDP Aktivierung:	Wenn diese Option aktiviert ist, wird RCCMD automatisch einen UDP Lauscher Socket anstelle des TCP Socket öffnen. Dies ermöglicht dem RCCMD Lauscher, RCCMD Broadcasts zu empfangen. Mögliche Werte sind “true” oder “false”, der Standard ist “true”.
Timeout:	Zeitüberschreitung für TCP Verbindungen. Der Standard ist 10 Sekunden. Es ist eigentlich nicht notwendig, diese Einstellung zu ändern.

Um alle Werte auf die Standardwerte zurückzusetzen, wählen Sie [Default] mit einem Klick auf [Tab] und drücken Sie [Enter].

Um die Maske zu verlassen, wählen Sie entweder [Ok] (Werte akzeptieren wie dargestellt) oder [Cancel] (alle Änderungen verwerfen).

Konfiguration der “Access Control List”

“Access Control List” beinhaltet eine Liste von gültigen Sender Adressen. Eine gültige Sender Adresse ist die IP-Adresse von einem RCCMD Sender, der berechtigt ist, eine Verbindung zu einem RCCMD Lauscher herzustellen.

Achtung: **Eine leere “Access Control List” bedeutet, dass jeder berechtigt ist, eine Verbindung herzustellen.**

Um zwischen den Einträgen in der Liste hin- und herzuwechseln, benutzen Sie die [↑] und [↓] Tasten. Um einen Eintrag auszuwählen, drücken Sie [Enter].

Abb. 129: Hinzufügen RCCMD UNIX Sender

Um eine IP-Adresse hinzuzufügen, drücken Sie [Tab], bis [Add] markiert ist, und drücken Sie [Enter].

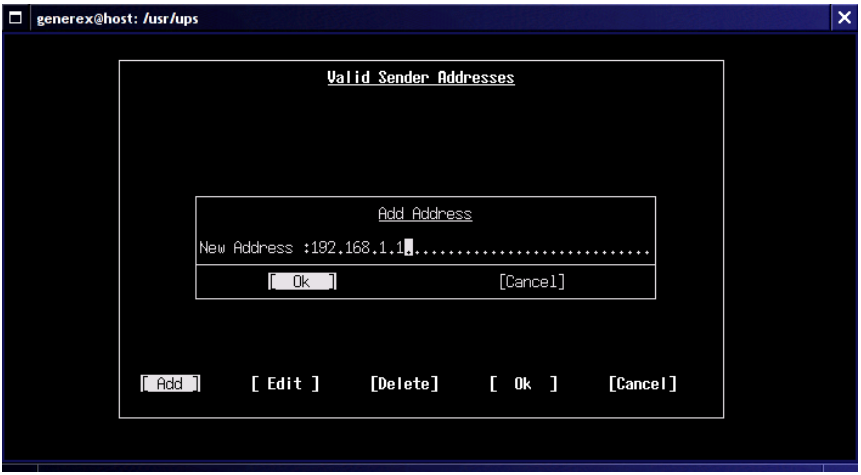

Abb. 130: RCCMD UNIX Sender Beispiel

Tragen Sie die IP-Adresse von der Workstation ein, die in der Lage sein soll, eine Verbindung herzustellen, dann drücken Sie [Enter].

Abb. 131: RCCMD UNIX Sender Überblick

Um einen Eintrag zu editieren, wählen Sie mit [↑] und [↓], bis der gewünschte Eintrag markiert ist. Danach drücken Sie [Tab] bis [Edit] markiert ist und drücken [Enter].

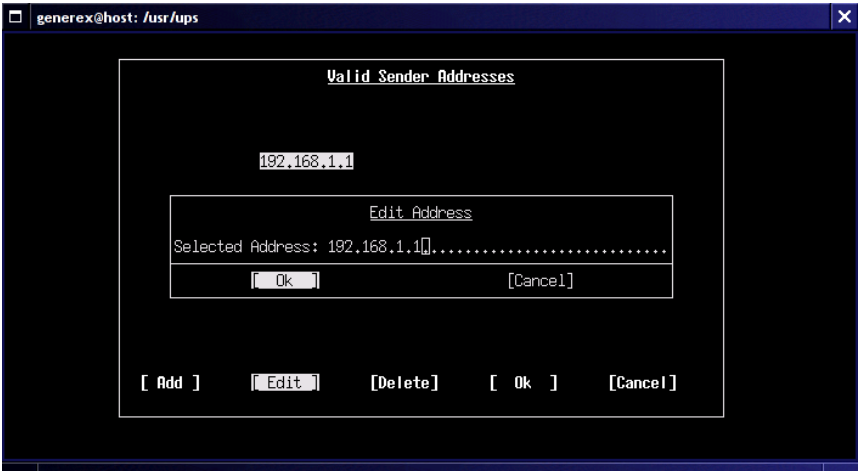

Abb. 132: RCCMD UNIX Sender Editierung

Sie können die Adresse im “Edit Address” Fenster editieren. Um Ihre Veränderungen zu speichern, wählen Sie [Ok] und drücken [Enter], andererseits [Cancel].

Um einen Eintrag in der Liste zu löschen, nutzen Sie die [↑] und [↓] Tasten, bis der gewünschte Eintrag markiert ist, drücken [Delete] und [Enter].

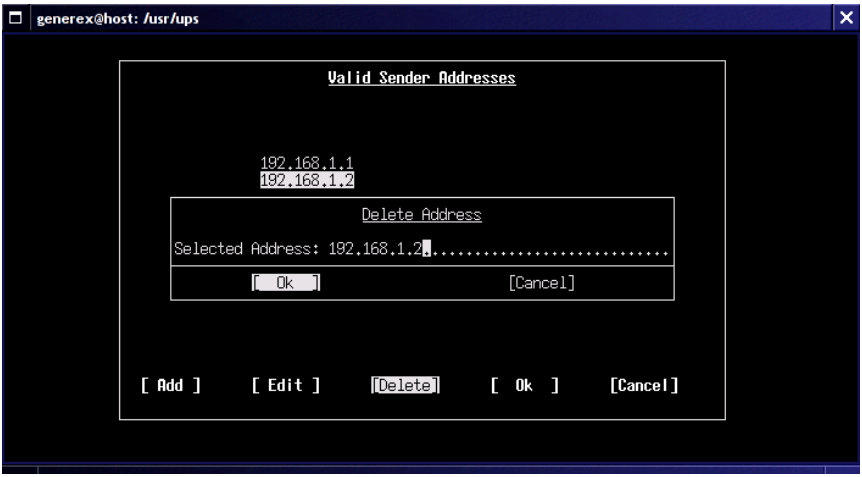

Abb. 133: RCCMD UNIX Sender Löschen

Bestätigen Sie das Löschen des Eintrags mit [Ok] und [Enter]. Um die Maske zu verlassen, wählen Sie entweder [Ok] (Werte akzeptieren wie dargestellt) oder [Cancel] (alle Änderungen verwerfen).

Netzwerkabfrage nach UPSMAN/UPSTCP:

Dieses Fenster bietet die Möglichkeit, das Netzwerk nach UPSMAN/UPSTCP Servern abzusuchen. Sie sollten die ermittelten IP-Adressen zu Ihrer “Access Contrtol List” hinzufügen.

Hinweis: **Die Optionen in diesen Fenstern beeinflussen RCCMD nicht direkt, aber die Ergebnisse der Netzwerkabfrage sollten in die “Access Control List” eingetragen werden.**

Abb. 134: RCCMD UNIX Sender Scan

lowest/highest IP:	Beim Start versucht die rccmd_conf, die primäre IP-Adresse des Hosts zu ermitteln. Von dieser Adresse wird ein korrespondierender Klasse C Netzwerkbereich abgeleitet. Dies sind die Standard Begrenzungen für eine Netzwerkabfrage. Wenn Sie ein anderes Netzwerk abfragen möchten oder den Bereich abstimmen möchten, verändern Sie in den “Scan Options” die Adressen (lowest and/or highest IP address).
Port to scan:	Der Port, zu dem sich der Scanner versucht zu verbinden. Der Standard Port ist 5769, gleichzeitig der Standard Port des UPSMAN/UPSTCP Servers. Wenn Sie den UPSMAN/UPSTCP auf einem anderen Port laufen haben, sollten Sie den Standard Port zur Abfrage dementsprechend ändern.

Um die Abfrage zu starten, wählen Sie [Scan] und drücken [Enter], andererseits [Cancel].

Konfiguration “Check Upsman/Upstcp”:

Der RCCMD Lauscher hat die Fähigkeit, den “Alive Check” zum UPSMAN/UPSTCP Servers periodisch durchzuführen.

Hinweis: **Das “Check UPSMAN/UPSTCP Feature ist nur verfügbar, wenn Sie mindestens eine Adresse in der “Access Control List” eingetragen haben.**

Wenn Sie mehrere Adressen in der Liste eingetragen haben, erscheint folgendes Pop-Up-Fenster:

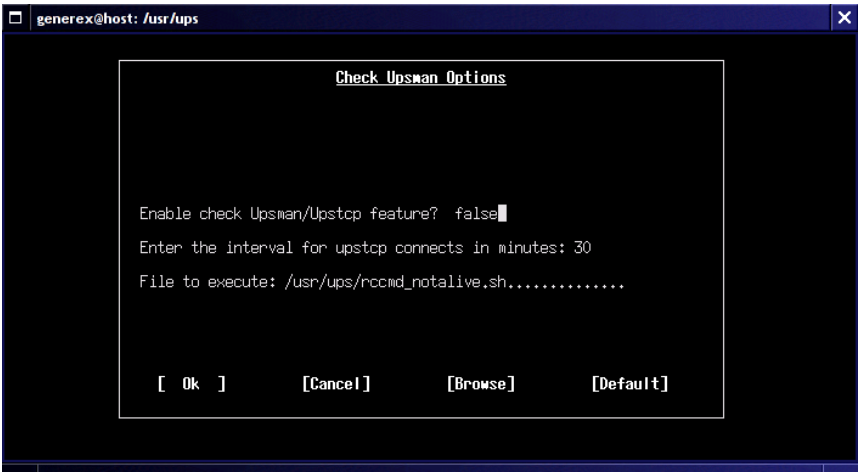

Abb. 135: RCCMD UNIX Check Upsman

Benutzen Sie [Tab], um sich zwischen den Options-Feldern und Buttons zu bewegen.

Enable check Upsman/Upstcp feature: Mögliche Werte sind “true” oder “false”, “false” ist Standard. Um den Wert zu verändern, nutzen Sie [↑] und [↓].

Enter the interval for upstcp connects in minutes:

Intervall-Angabe in Minuten. Der Standard ist 30 Minuten. Um diesen Wert zu verändern, überschreiben Sie den Wert im Options-Feld.

File to execute: Dieses File wird ausgeführt, wenn RCCMD nicht in der Lage ist, eine Verbindung zu einem oder mehreren UPSMAN/UPSTCP Servern herzustellen, in der Annahme, das entweder der HOST unten ist oder der UPSMAN/UPSTCP Dienst nicht läuft. Standard ist “/usr/ups/rccmd_notalive.sh”. Wenn Sie diesen Wert verändern möchten, überschreiben Sie den String im Optionen-Feld oder mit der Auswahl eines Files. Um den File-Browser zu aktivieren,

drücken Sie [Tab] bis [Browse] markiert ist und drücken [Enter].

Um alle Werte auf die Standardwerte zurückzusetzen, wählen Sie [Default] mit einem Klick auf [Tab] und drücken Sie [Enter].

Um die Maske zu verlassen, wählen Sie entweder [Ok] (Werte akzeptieren wie dargestellt) oder [Cancel] (alle Änderungen verwerfen).

Konfiguration der “Logfile Options”:

Der RCCMD Lauscher ist in der Lage, ein Log File zu schreiben und es zu pflegen/warten. Es loggt Events wie Start/Stopp des Programms, akzeptierte und abgelehnte Netzwerk Verbindungen und ausgeführte Befehle/Files. Einige Parameter können Sie in den Log File Optionen eintragen:

Abb. 136: RCCMD UNIX Log File Optionen

Enable logging to file:	Mögliche Werte sind “true” oder “false”, “false” ist Standard. Um den Wert zu verändern, nutzen Sie [↑] und [↓].
Select maximum size of log file:	Das Log File wird nicht größer sein als dieser Wert. Wenn es dieses Limit überschreiten würde, würde RCCMD es erst um 10% verkleinern, um dann mit dem Loggen fortzufahren. Das Log File wird vom Start verkleinert, sodass ältere Einträge zuerst gelöscht werden würden. Die Standard Größe ist 1024 Kb. Um diesen Wert zu verändern, nutzen Sie [↑] und [↓]. Der Spezial-Wert “0” bedeutet, dass das File nicht verkleinert oder überschrieben werden würde.

Log file name:	Diese Option spezifiziert den Namen und dien Ort des Log Files. Der Standard ist “/usr/ups/rccmd.log”. Wenn Sie diesen Wert verändern möchten, überschreiben Sie den String im Optionen-Feld oder mit der Auswahl eines Files. Um den File-Browser zu aktivieren, drücken Sie [Tab] bis [Browse] markiert ist und drücken [Enter].

Um alle Werte auf die Standardwerte zurückzusetzen, wählen Sie [Default] mit einem Klick auf [Tab] und drücken Sie [Enter].

Um die Maske zu verlassen, wählen Sie entweder [Ok] (Werte akzeptieren wie dargestellt) oder [Cancel] (alle Änderungen verwerfen).

Konfiguration der “Shutdown Options”:

Abb. 137: RCCMD UNIX Shutdown Optionen

File to execute:	Dieses File wird ausgeführt, wenn RCCMD den “Shutdown” Befehl empfängt. Standard ist “/usr/ups/rccmd_shutdown.sh”

Um alle Werte auf die Standardwerte zurückzusetzen, wählen Sie [Default] mit einem Klick auf [Tab] und drücken Sie [Enter].

Um die Maske zu verlassen, wählen Sie entweder [Ok] (Werte akzeptieren wie dargestellt) oder [Cancel] (alle Änderungen verwerfen).

Beenden der rccmd_conf:

In der Hauptkonfiguration “RCCMD Configuration” wählen Sie entweder [Save] oder [Exit] und drücken [Enter]. Save bedeutet, dass rccmd.cfg wird mit seinen aktuellen Werten, die Sie auf dem Bildschirm sehen, gespeichert. Mit Exit verlassen Sie das Programm, ohne die rccmd.cfg berührt zu haben.

Der File Browser:

Einige der Konfigurations-Masken nutzen einen integrierten File Browser:

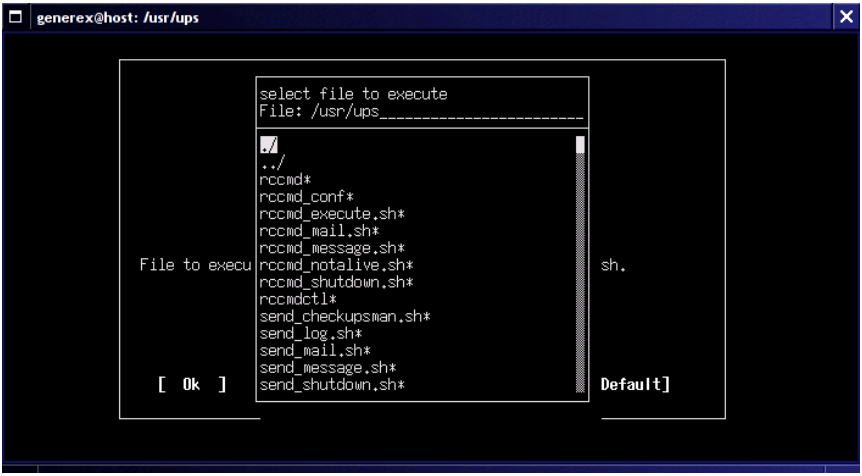

Abb. 138: RCCMD UNIX File Browsing

Die [↑] und [↓] Tasten können zum Bewegen in der Liste genutzt werden. Mit dem Drücken von [Enter] wählen Sie den markierten Eintrag aus. Wenn der ausgewählte Eintrag ein Verzeichnis ist, wird der Browser das Verzeichnis und seine Inhalte auflisten. Dateitypen können mit den Eingaben “ls-F” angezeigt werden. Sternchen “*” bedeuten auszuführende Dateien, Schrägstriche “/” für Verzeichnisse, “@” für symbolische Links und Gleichheitszeichen “=” für Sockets.

UNIX RCCMD multiple Sender Konfiguration :

Wenn Sie mehr als eine Sender-Adresse verwenden möchten, sollte die rccmd.sh wie folgt modifiziert werden:

```
#! /bin/sh

# You may specify a sender IP to accept signals from,
# default is everyone.
SENDER="-a 10.55.52.82 -a 10.55.52.83 -a 10.55.52.84"

# You may change the port to listen on,
# default is 6003.
PORT=
```

# You must define a command to be executed upon
# receiving signal.
SCRIPT=/usr/ups/doshutdown.sh

test -z $SENDER || SENDER="-a $SENDER"
test -z $PORT || PORT="-p $PORT"
to start:
./rccmd -l $SENDER $PORT $SCRIPT

UNIX RCCMD multiple Sender Konfiguration (V3 und höher):

Wie starte ich den Rccmd V3 mehrfach über verschiedene Ports auf einer UNIX Maschine?
Dafür muss jedes RCCMD einen eigenen TCP-Port bekommen, z.B.:

```
./rccmd –l –p 6003
./rccmd –l –p 6004
./rccmd –l –p 6005
```

Import in die RC Files:

Am einfachsten wäre es, eine entsprechende Anzahl neuer Startskripte anzulegen und diese dann durch das alte aufzurufen, z.B.:

1) Neue Startskripte erzeugen:
Dazu altes Skript dreimal kopieren und dabei umbennenen:

```
cp rccmdctl.sh rccmdctl-1.sh
cp rccmdctl.sh rccmdctl-2.sh
cp rccmdctl.sh rccmdctl-3.sh
```

2) Neue Startskripte anpassen:
Dazu in jedem der drei neuen Skripte durch die Variable 'RCCMDPORT' den TCP-Port anpassen:

```
...
   RCCMDPORT=6003
...
```

3) Altes Startskript anpassen, damit dieses die neuen Skripte nachstartet.
Dazu mindestens den 'start' und den 'stop' -Zweig in der Datei 'rccmdctl' ersetzen:

```
 start)
     /usr/ups/rccmdctl-1.sh start
     /usr/ups/rccmdctl-2.sh start
     /usr/ups/rccmdctl-3.sh start
   ;;

   stop)
     /usr/ups/rccmdctl-1.sh stop
     /usr/ups/rccmdctl-2.sh stop
     /usr/ups/rccmdctl-3.sh stop
   ;;
```

ACHTUNG: **Diese Skripte NICHT mit einem Windows-Editor bearbeiten, dann werden diese wegen der unterschiedlichen Zeilenumbrüche auf Windows/Unix zerstört!**

4. RCCMD auf VMware

VMware ist Hersteller für Virtualisierungslösungen und vertreibt verschiedene Ausprägungen solcher Produkte. RCCMD kann neben den virtuellen Systemen auch die VMware physikalischen Systeme herunterfahren.

4.1 RCCMD auf VMware ESX

Die RCCMD Software auf VMware ESX ist ein auf Linux basierter TCP Client, der das Empfangen von Shutdown Signalen von der UPSMAN Software, CS121 SNMP Adapter oder jeder anderen lizensierten RCCMD Anwendung ermöglicht.

RCCMD auf VMware ESX läuft auf GNU Linux 2.6.18 oder höher, das die Basis der VMware ESX Plattform ist.

Für die Installationsanleitung von RCCMD schauen Sie bitte in das Kapitel 5. RCCMD auf UNIX. Im Folgenden beschreiben wir nur die speziellen Aspekte, die nur VMware ESX relevant sind.

Installation:

Da der VMware ESX keine grafische Oberfläche besitzt, empfehlen wir, eine lokale Schnittstelle, z. B. ein CD-ROM Laufwerk, auf Ihrem VMware ESX zu nutzen oder mit einem USB Stick zu arbeiten um RCCMD zu installieren.

- Laden Sie RCCMD mit ihrer Lizenznummer (nicht älter als 2 Jahre) von der GENEREX Webseite herunter, und extrahieren Sie das TAR File. Kopieren Sie die Files auf eine CD-R, und legen Sie die CD in das Laufwerk auf Ihrem ESX Server. Alternativ können Sie die UPSMAN CD-ROM Version 5.48 oder höher nutzen.
- Loggen Sie sich als Root ein, und mounten Sie die CD-ROM auf Ihrem VMware ESX Computer: Geben Sie `mount/dev/cdrom` ein.
- Wechseln Sie zu dem CD-ROM Verzeichnis mit: `cd/mnt/cdrom` – mit `ls` können Sie sich die Files der CD-ROM anzeigen lassen. Wechseln Sie in das Verzeichnis DRIVERS/PreviousVersions/UNIX-ALL (UPSMAN CD-ROM). Darin befindet sich das Installations-File “install”.
- Starten Sie die Installation mit der Eingabe: `./install` und folgen Sie den Anweisungen auf dem Bildschirm, die identisch zur Installation von RCCMD auf UNIX ist.
- Nach dem die Installation beendet ist, wird ein neuer Prozess auf Ihrem VMware ESX laufen: `:/rccmd -l` , was bedeutet, dass das System nun bereit ist.

- **Achtung:** Der VMware ESX hat standardmässig eine aktive Firewall, die keine RCCMD Signale zulässt.

Firewall Konfiguration:

Die folgende Firewall Konfiguration auf dem VMware ESX ist erforderlich, um RCCMD Signale empfangen zu können:

```
esxcfg-firewall –o 6003,tcp,in,RCCMD
```

Starten Sie den Firewall Service neu, um Ihre Einstellungen zu speichern:

```
service firewall restart
```

RCCMD ist nun im Client-Modus konfiguriert und wird das File *shutdown.sh* auf Ihrem VMware ESX starten, wenn ein CS121 Adapter oder UPSMAN ein RCCMD Shutdown Signal sendet. Das File *shutdown.sh* führt ein *init 0 shutdown* auf Ihrem VMware ESX aus. Ändern Sie das File, wenn Sie eine andere Shutdown Prozedur verwenden möchten.

Hinweis: **Es wird empfohlen, RCCMD auch auf den virtuellen Gast-systemen zu installieren und diese VOR dem physikalischen Hostrechner herunterzufahren. Dies garantiert ein sauberes Herunterfahren der virtuellen Maschinen und verhindert den möglichen Datenverlust durch ein nicht erfolgreiches Hibernating.**

4.2 RCCMD auf VMware ESXi 4.x – 5.x

Die RCCMD Software auf VMware ESXi ist ein auf Linux basierter TCP Client (TCP/IP Empfänger), der das Empfangen von Shutdown Signalen von der UPSMAN Software, CS121 SNMP Adapter oder jeder anderen lizensierten RCCMD Anwendung ermöglicht.

Folgende Voraussetzungen sind für die Installation und Konfiguration von RCCMD auf VMWare ESXi erforderlich:

1. Ein VMWare vSphere Client muss auf einer Windows Workstation installiert sein.

2. Auf dem ESXi Hypervisor muss in einer virtuellen Maschine eine vMA installiert und konfiguriert werden. Die vMA kann von VMware als Download geladen werden. Lesen Sie dazu in der VMware Dokumentation, z. B. für die vMA 4 im folgenden Link ab Seite 13 : http://www.vmware.com/support/developer/vima/vma41/doc/vma_41_guide.pdf. (Neuere vMA 5 entsprechend.)

3. Ein SCP/SFTP Client wird benötigt, um die RCCMD Installationsdateien auf der vMA kopieren zu können (z. B. „Filezilla“ oder jeder andere SFTP Client), und es wird ein Terminalprogramm benötigt (z. B. Putty), um eine Kommandozeile auf der vMA zu öffnen. Beide Tools gehören zum üblichen

Werkzeug eines ESXi Servers oder jedes anderen UNIX Systems und werden daher in diesem Handbuch nicht weiter beschrieben.

4. Anzahl an RCCMD VMware Client Lizenzen (mindestens 1 Lizenz).

vSphere Client: Dies ist ein grafisches Verwaltungstool für ESXi Server. Wir gehen von einer bestehenden Installation eines vSphere Clients aus und verzichten auf die Beschreibung dieser Installation und dessen Bedienung

vMA: Der VMware ESXi Server bietet den vSphere Management Assistant (vMA) 4.x oder 5.x als Schnittstelle für externe Anwendung an, in welcher der RCCMD Client läuft. D.h. der RCCMD Client in der vMA erhält Signale zum Shutdown vom CS121 und sendet das Shutdown Kommando an den ESXi Server über die vMA Schnittstelle weiter.

Der vMA Assistant bietet ein Management-Interface an, mit dem der VMware ESXi automatisch per Skript gesteuert werden kann.

Auf der vMA wird RCCMD installiert. Dabei erkennt der RCCMD-Installer automatisch, dass die Installation auf einer VMware Anwendung ausgeführt wird und installiert entsprechend angepasste Scriptdateien für den Shutdown.

Achtung: **OEM Versionen der VMware, die nicht dem Verhalten des Originals entsprechen, werden von uns nicht unterstützt!**

4.2.1 ESXi Host Konfiguration über die vMA und vSphere

RCCMD wird in der vMA installiert, und über vSphere wird der Shutdown auf den betreffenden ESXi Hosts konfiguriert. Dazu sendet der RCCMD den Shutdownbefehl von der vMA an den ESXi Host. Das folgende Bild zeigt den RCCMD Client installiert in der vMA, von wo aus der Shutdown auf den/die ESXi Hosts eingeleitet wird.

Mit dem vSphere-Client kann jeder Host so konfiguriert werden, dass dieser vor dem Herunterfahren seine Gastsysteme sauber herunterfährt. Auf den virtuellen Maschinen müssen hierfür die VMware-Tools installiert sein, um diese Funktion nutzen zu können.

4.2.2 Shutdown Konfiguration virtuelle Maschinen auf dem ESXi

Wählen Sie im vSphere-Client Ihren Host (1) aus, klicken Sie auf “Konfiguration” (2), und markieren Sie “VM starten/herunterfahren” (3). Klicken Sie nun auf vMA (4) und oben rechts auf “Eigenschaften (5).

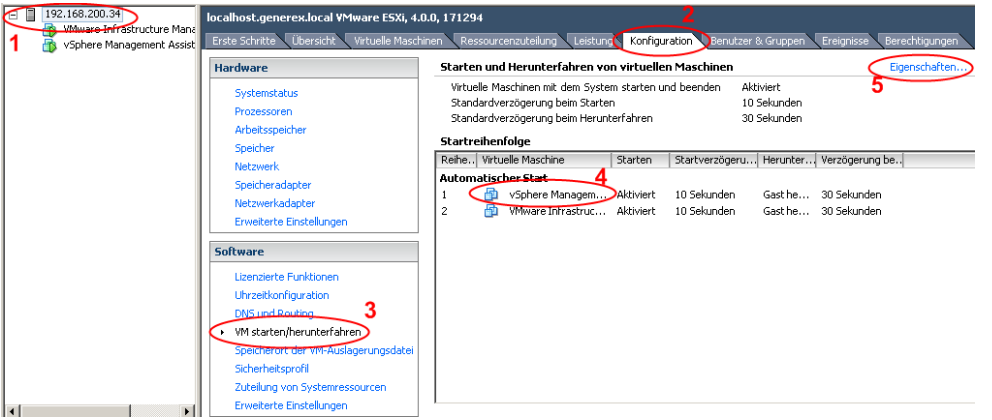

Abb. 139: vSphere-Client Konfiguration

Wählen Sie im Eigenschaften-Dialog den vMA aus, und setzen Sie seine Werte wie abgebildet auf 10 Sekunden Startverzögerung und 30 Sekunden Verzögerung beim Herunterfahren.

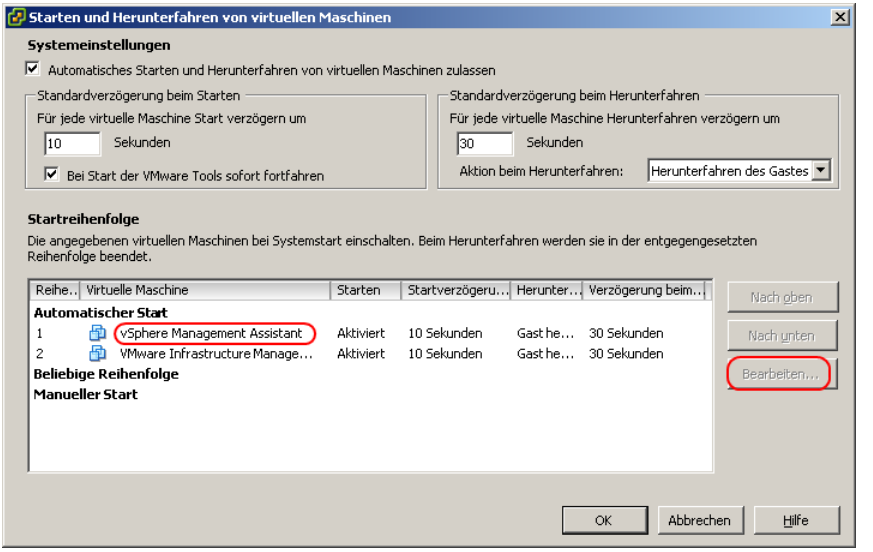

Abb. 140: vSphere-Client Autostart-Konfiguration

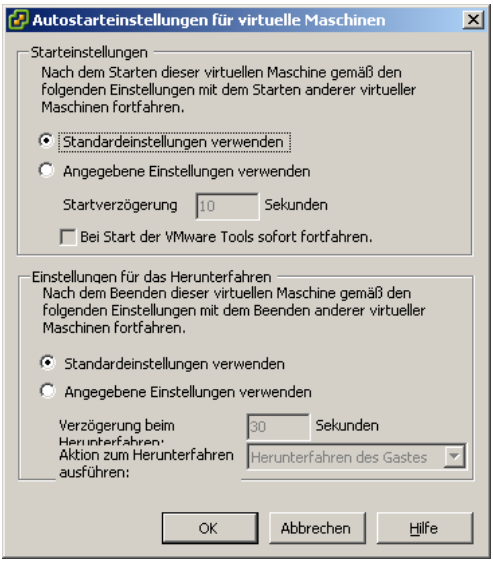

Abb. 141: vSphere-Client- Autostart-Verzögerung

Im folgenden Bild sehen Sie die Konfigurationsmöglichkeiten über den vSphere Client:

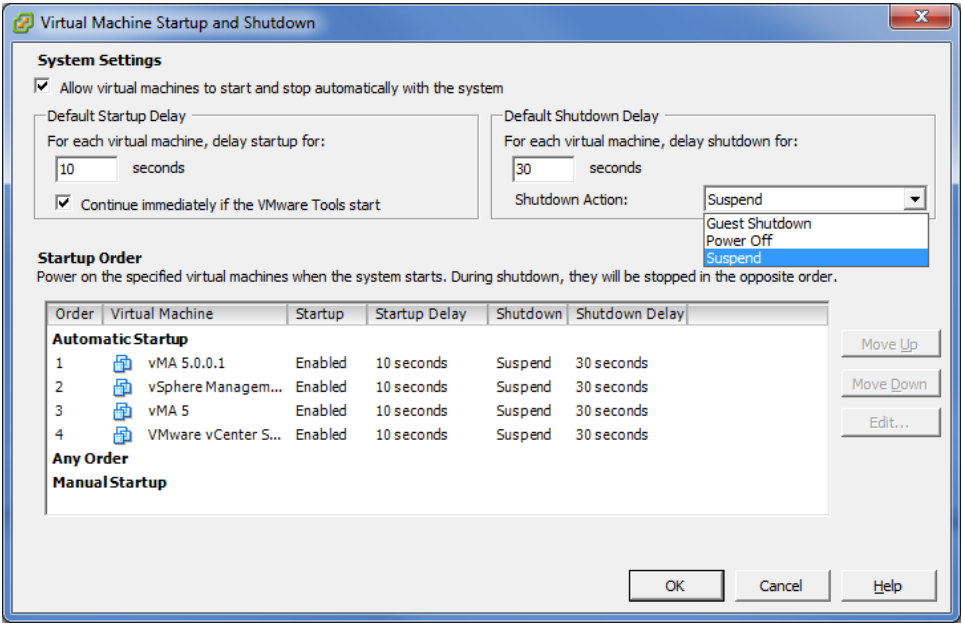

Abb. 142: vSphere-Client – Startup and Shutdown

Folgende Shutdown Actions stehen zur Verfügung:

- Power Off = AUSSCHALTEN (ohne Shutdown)
- Guest Shutdown = (nur wenn in der jeweiligen virtuellen Maschine die VMware Tools installiert wurden!) Shutdown des Betriebssystems
- Suspend = Hibernating oder Sleep Mode, die VMs werden angehalten

Hinweis:

Ein Shutdown über die VMWare Tools unter Nutzung der Funktionen „Guest Shutdown“, „Suspend“ oder „Power OFF“ garantiert allerdings nicht, dass die damit heruntergefahrenen Gast-Betriebssysteme auch ohne Datenverlust neustarten. Um dieses geringe Risiko auszuschliessen, kann auf jedem virtuellen Betriebsystem zusätzlich RCCMD installiert werden und VOR dem ESXi Host per RCCMD Shutdown herunterzufahren. Dies empfiehlt sich inbesondere bei Datenbanken.

Die Verzögerungszeiten für die Gastsysteme/virtuellen Maschinen die auf dem ESXi laufen und mit dem Host heruntergefahren werden sollen, können abweichen und müssen individuell eingerichtet werden. Die Dauer, die der Server dann für den Shutdown benötigt, wird dadurch enstprechend vergrössert.

Die Funktion, die Gastsysteme herunterzufahren, wird an den ESXi Host übertragen. Es gibt virtuelle Maschinen, die voneinander abhängig sind und daher in einer genauen Reihenfolge heruntergefahren werden müssen. Diese Reihenfolge und die gewünschten Aktionen (Herunterfahren der jeweiligen Gastsysteme) müssen vom Administrator im ESXi Host konfiguriert werden. RCCMD sendet das Shutdown-Signal an den Host, der dann die konfigurierten Aktionen ausführt.

4.2.3 RCCMD Installation auf der vMA

Verwenden Sie ihre RCCMD Client-Lizenznummer, und laden Sie sich von der Website des USV Herstellers oder von www.generex.de den RCCMD client für VMware ESXi herunter. RCCMD wird im Download als sogenannte „TAR“ Datei geliefert. Kopieren Sie die Datei rccmdinst.tar mit Hilfe des SCP Clients (SFTP) auf die vMA. Einen SFTP Client kann als Freeware aus dem Internet verwendet werden, z. B. Filezilla oder ein ähnliches Tool kann die Funktion der Überrtragung des RCCMD Pakets auf das Zielsystem ausführen.

- Loggen Sie sich auf der vMA ein. Für das Einloggen auf der vMA wird ein Terminalprogramm benötigt, z. B. Putty oder einer anderen Terminalsoftware.
- Erstellen Sie z. B. mit „mkdir“ ein temporäres Verzeichnis z. B. mit dem Namen „RCCMD“, wohin Sie dann die TAR Datei hineinkopieren.
- Entpacken Sie die tar-Datei mit dem Befehl: „`tar –xvf rccmdinst.tar`“

Es entstehen folgende Dateien nach dem Entpackvorgang:

```
[root@vMA41 ~]# cd /home/vi-admin/
[root@vMA41 ~]# mv RCCMD/ tmp
[root@vMA41 ~]# ls
rccmdinst.tar  tmp
[root@vMA41 ~]# mkdir RCCMD
[root@vMA41 ~]# mv rccmdinst.tar RCCMD/
[root@vMA41 ~]# cd RCCMD/
[root@vMA41 RCCMD]# tar -xvf rccmdinst.tar
gpg-pub.txt
installer.info
installer.properties
installRCCMD.bin
installRCCMD.bin.asc
installRCCMD.bin.md5
versionOEM12.xml
[root@vMA41 RCCMD]# ls
gpg-pub.txt     installer.properties  installRCCMD.bin.asc  rccmdinst.tar
installer.info  installRCCMD.bin      installRCCMD.bin.md5  versionOEM12.xml
[root@vMA41 RCCMD]#
```

Abb. 143: Installationsvorbereitung

Sie sollten als „root“ eingeloggt sein und damit Administratorrechte besitzen.

Starten Sie die Installation mit dem Aufruf: `./installRCCMD.bin`

```
[root@vMA41 ~]# ls
RCCMD
[root@vMA41 ~]# cd RCCMD/
[root@vMA41 RCCMD]# ./installRCCMD.bin
```

Abb. 144: Ausführung der Binärdatei installRCCMD.bin und Beginn des Installationsskriptes

Alternativ können Sie auch mit dem „Sudo-Befehl“ als vi-admin installieren:

```
sudo ./installRCCMD.bin
```

Wählen Sie die Sprache aus, und drücken Sie die Eingabetaste.

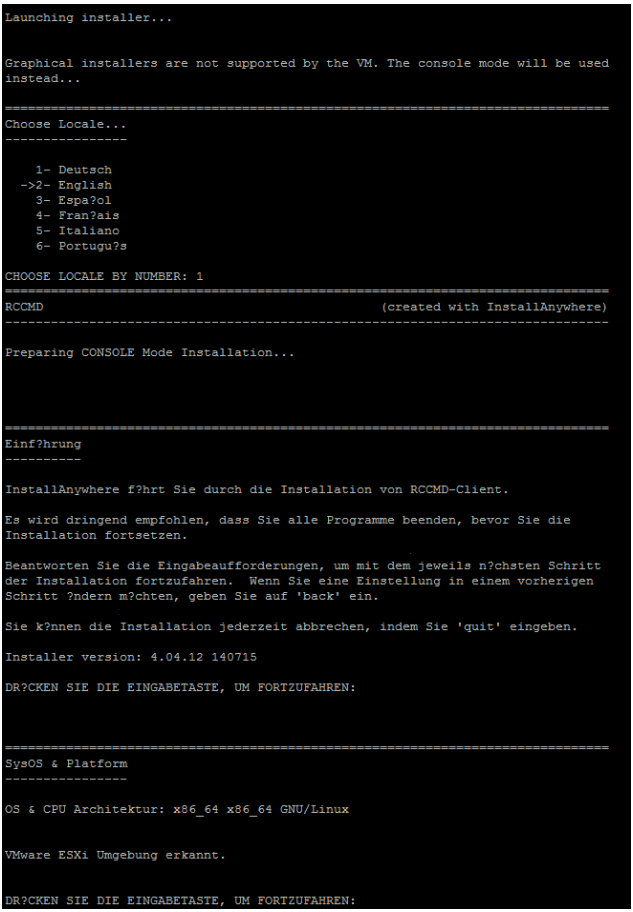
Launching installer...
Graphical installers are not supported by the VM. The console mode will be used instead...
Choose Locale...
1- Deutsch
->2- English
3- Espa?ol
4- Fran?ais
5- Italiano
6- Portugu?s
CHOOSE LOCALE BY NUMBER: 1
RCCMD
(created with InstallAnywhere)
Preparing CONSOLE Mode Installation...
Einf?hrung
InstallAnywhere f?hrt Sie durch die Installation von RCCMD-Client.
Es wird dringend empfohlen, dass Sie alle Programme beenden, bevor Sie die Installation fortsetzen.
Beantworten Sie die Eingabeaufforderungen, um mit dem jeweils n?chsten Schritt der Installation fortzufahren. Wenn Sie eine Einstellung in einem vorherigen Schritt ?ndern m?chten, geben Sie auf 'back' ein.
Sie k?nnen die Installation jederzeit abbrechen, indem Sie 'quit' eingeben.
Installer version: 4.04.12 140715
DR?CKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:
SysOS & Platform
OS & CPU Architektur: x86_64 x86_64 GNU/Linux
VMware ESXi Umgebung erkannt.
DR?CKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 145: Sprachauswahl und Beginn der Installation - die Meldung „Recognized VMware ESXi environment“ zeigt an, dass die richtige Hardware erkannt wurde

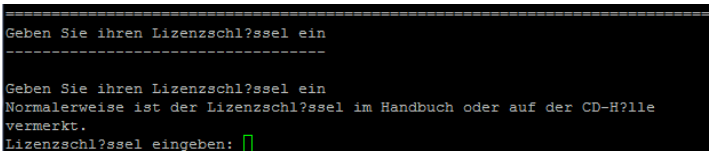
Geben Sie ihren Lizenzschl?ssel ein
Geben Sie ihren Lizenzschl?ssel ein
Normalerweise ist der Lizenzschl?ssel im Handbuch oder auf der CD-H?lle vermerkt.
Lizenzschl?ssel eingeben:

Abb. 146: Lizenz Eingabe

Geben Sie den RCCMD Lizenzschlüssel ein. Wählen Sie die Produkt Features, die Sie installieren möchten.

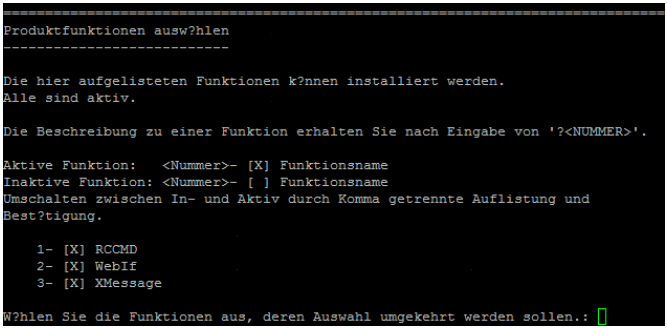
Produktfunktionen ausw?hlen
Die hier aufgelisteten Funktionen k?nnen installiert werden.
Alle sind aktiv.
Die Beschreibung zu einer Funktion erhalten Sie nach Eingabe von '?<NUMMER>'.
Aktive Funktion: <Nummer>- [X] Funktionsname
Inaktive Funktion: <Nummer>- [ ] Funktionsname
Umschalten zwischen In- und Aktiv durch Komma getrennte Auflistung und
Best?tigung.
1- [X] RCCMD
2- [X] WebIf
3- [X] XMessage
W?hlen Sie die Funktionen aus, deren Auswahl umgekehrt werden sollen.:

Abb. 147: Produkt Feature Auswahl

4.2.3.1 RCCMD Installation ohne vCenter

Danach geben Sie bitte an, ob sich ein vCenter in Ihrer VMware Umgebung befindet und den Hostnamen oder die IP-Adresse des ESXi Servers.

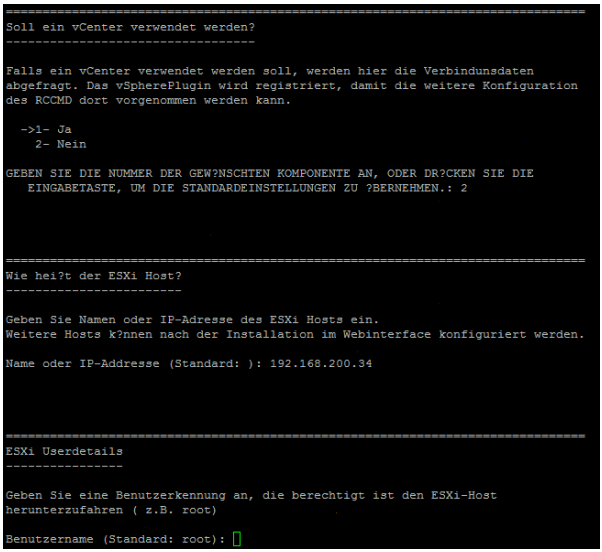
Soll ein vCenter verwendet werden?
Falls ein vCenter verwendet werden soll, werden hier die Verbindunsdaten
abgefragt. Das vSpherePlugin wird registriert, damit die weitere Konfiguration
des RCCMD dort vorgenommen werden kann.
->1- Ja
2- Nein
GEBEN SIE DIE NUMMER DER GEW?NSCHTEN KOMPONENTE AN, ODER DR?CKEN SIE DIE
EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ?BERNEHMEN.: 2
Wie hei?t der ESXi Host?
Geben Sie Namen oder IP-Adresse des ESXi Hosts ein.
Weitere Hosts k?nnen nach der Installation im Webinterface konfiguriert werden.
Name oder IP-Addresse (Standard:): 192.168.200.34
ESXi Userdetails
Geben Sie eine Benutzerkennung an, die berechtigt ist den ESXi-Host
herunterzufahren (z.B. root)
Benutzername (Standard: root):

Abb. 148: Interaktive Eingaben – vCenter, ESXi Server Hostname oder IP-Adresse

Geben Sie die Zeit an, die für den Shutdown der virtuellen Maschinen benötigt wird und weitere Details.

```
================================================================================
Wie gro? ist die Herunterfahrzeit?
---------------------------------

Geben Sie die Dauer in Sekunden an, die alle virtuellen Maschinen auf dem Host
zum herunterfahren ben?tigen.

Herunterfahrzeit (Standard: 90):




================================================================================
Wie hei?t diese VM
------------------

Geben Sie den Namen dieser VM an, so wie er im vSphere Client angezeigt wird.

vMA Name (Standard: ): vMA_5.5_ES
```

Abb. 149: Interaktive Eingaben – Herunterfahrzeit, vMA Name

4.2.3.2 RCCMD Installation mit vCenter

Geben Sie die Zugangsdaten für das vCenter ein.

```
================================================================================
Soll ein vCenter verwendet werden?
----------------------------------

Falls ein vCenter verwendet werden soll, werden hier die Verbindunsdaten
abgefragt. Das vSpherePlugin wird registriert, damit die weitere Konfiguration
des RCCMD dort vorgenommen werden kann.

  ->1- Ja
    2- Nein

GEBEN SIE DIE NUMMER DER GEW?NSCHTEN KOMPONENTE AN, ODER DR?CKEN SIE DIE
   EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ?BERNEHMEN.:




================================================================================
Adresse des vCenter eingeben
----------------------------

Namen oder IP-Adresse des vCenter-Servers angeben.

Name oder IP-Adresse (Standard: ): 192.168.200.103

Benutzerame (Standard: root):




================================================================================
Passwort f?r root
-----------------

Passwort f?r root eingeben.

Bitte geben Sie das Kennwort ein:
```

Abb. 150: Interaktive Eingaben – vCenter Zugangsdaten

Es folgt die Installationsübersicht.

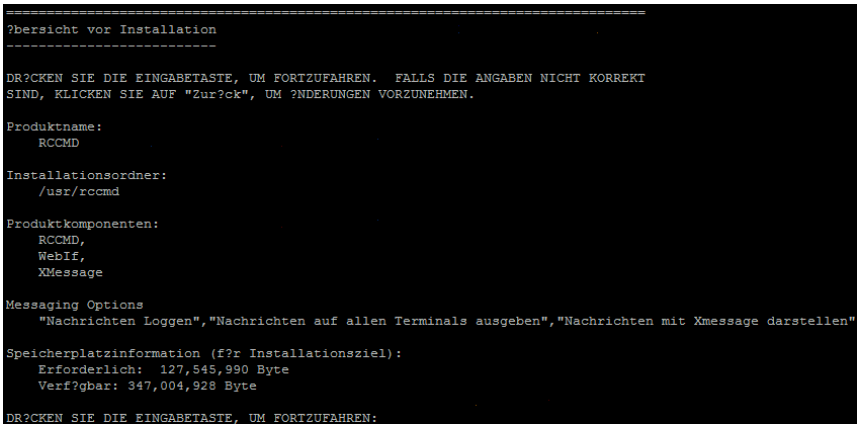

Abb. 151: Interaktive Eingaben – Installationsübersicht

Wählen Sie ein Protokoll und einen entsprechenden Port aus.

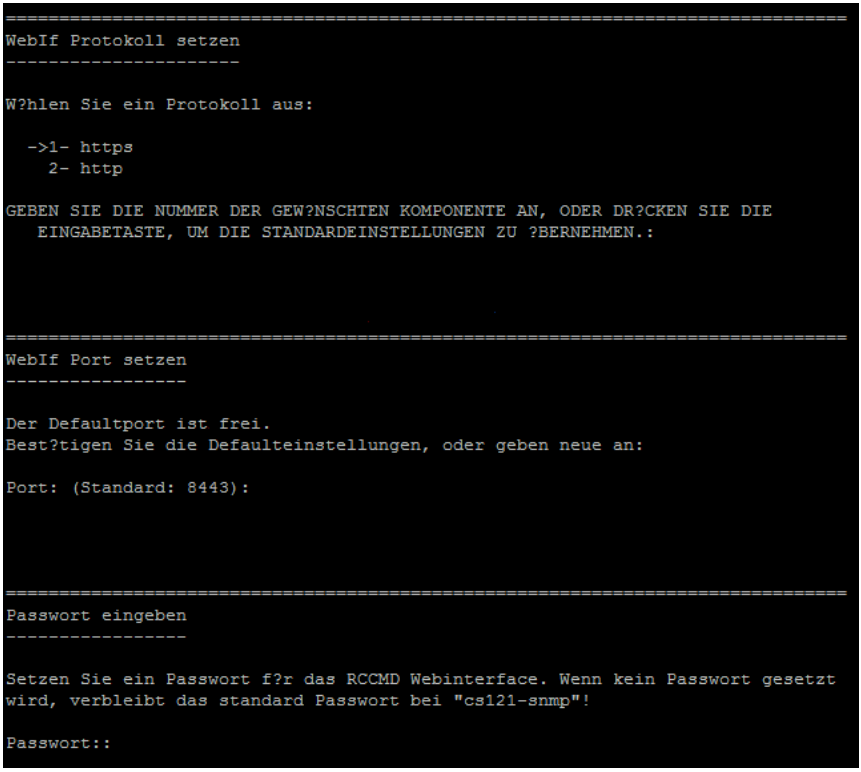
WebIf Protokoll setzen
W?hlen Sie ein Protokoll aus:
->1- https
2- http
GEBEN SIE DIE NUMMER DER GEW?NSCHTEN KOMPONENTE AN, ODER DR?CKEN SIE DIE
EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ?BERNEHMEN.:
WebIf Port setzen
Der Defaultport ist frei.
Best?tigen Sie die Defaulteinstellungen, oder geben neue an:
Port: (Standard: 8443):
Passwort eingeben
Setzen Sie ein Passwort f?r das RCCMD Webinterface. Wenn kein Passwort gesetzt
wird, verbleibt das standard Passwort bei "cs121-snmp"!
Passwort::

Abb. 152: Interaktive Eingaben – Portauswahl, Passworteingabe

Es folgt ein Hinweis, dass eine RCCMD Konfiguration erforderlich ist.

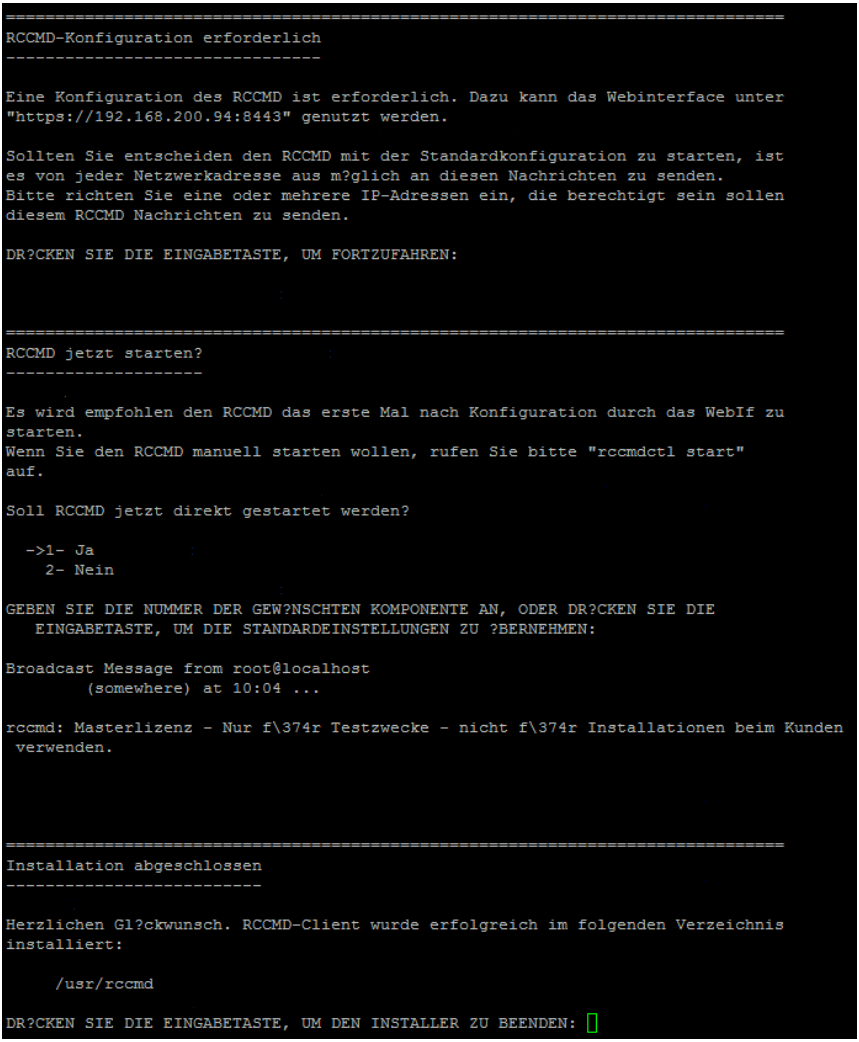
RCCMD-Konfiguration erforderlich
Eine Konfiguration des RCCMD ist erforderlich. Dazu kann das Webinterface unter
"https://192.168.200.94:8443" genutzt werden.
Sollten Sie entscheiden den RCCMD mit der Standardkonfiguration zu starten, ist
es von jeder Netzwerkadresse aus m?glich an diesen Nachrichten zu senden.
Bitte richten Sie eine oder mehrere IP-Adressen ein, die berechtigt sein sollen
diesem RCCMD Nachrichten zu senden.
DR?CKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:
RCCMD jetzt starten?
Es wird empfohlen den RCCMD das erste Mal nach Konfiguration durch das WebIf zu
starten.
Wenn Sie den RCCMD manuell starten wollen, rufen Sie bitte "rccmdctl start"
auf.
Soll RCCMD jetzt direkt gestartet werden?
->1- Ja
2- Nein
GEBEN SIE DIE NUMMER DER GEW?NSCHTEN KOMPONENTE AN, ODER DR?CKEN SIE DIE
EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ?BERNEHMEN:
Broadcast Message from root@localhost
(somewhere) at 10:04 ...
rccmd: Masterlizenz - Nur f\374r Testzwecke - nicht f\374r Installationen beim Kunden
verwenden.
Installation abgeschlossen
Herzlichen Gl?ckwunsch. RCCMD-Client wurde erfolgreich im folgenden Verzeichnis
installiert:
/usr/rccmd
DR?CKEN SIE DIE EINGABETASTE, UM DEN INSTALLER ZU BEENDEN:

Abb. 153: Interaktive Eingaben – Hinweis, Abschluss

Hinweis: **Die vMA wird zeitgleich mit dem ESXi Server heruntergefahren - dies Verhalten ist nicht kritisch für eine RCCMD vMA. Wenn im vCenter Server Programm vMotion aktiviert ist, dann wird die vMA automatisch auf einen anderen ESXi Server verschoben (die IP-Adresse und Funktionalität der vMA bleibt dabei erhalten).**

RCCMD überprüft während der Installation die Korrektheit der angegebenen Zugangsdaten. Wenn inkorrekt, erfolgt folgende Meldung.

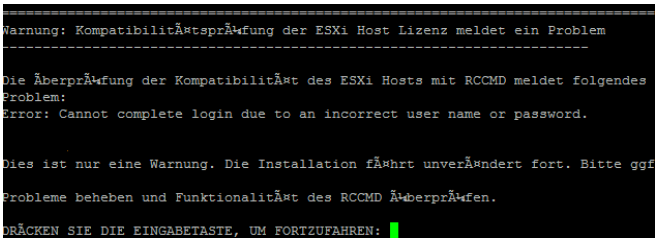
Warnung: KompatibilitÃ¤tsprÃ¼fung der ESXi Host Lizenz meldet ein Problem
Die ÃberprÃ¼fung der KompatibilitÃ¤t des ESXi Hosts mit RCCMD meldet folgendes Problem:
Error: Cannot complete login due to an incorrect user name or password.
Dies ist nur eine Warnung. Die Installation fÃ¤hrt unverÃ¤ndert fort. Bitte ggf
Probleme beheben und FunktionalitÃ¤t des RCCMD Ã¼berprÃ¼fen.
DRÃCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 154: Interaktive Eingaben – Warnung inkorrekter Zugangsdaten

Hinweis für vMA 4.x: Automatische Firewall Konfiguration

Achtung: **Nicht nötig auf VMware ESXi 5, da diese Version ohne Firewall ausgeliefert wird.**

RCCMD benötigt den Port 6003 (TCP und UDP) für eingehende IP-Pakete, bei Nutzung von „Check Alive“ Funktion auch TCP Port 5769 wird automatisch während der Installation freigeschaltet. Bei einer vMA 4 werden vom Installscript diese Ports automatisch freigeschaltet und ein entsprechendes Fenster zeigt diesen Vorgang an.

root@vMA41:~
Firewall geÃ¶ffnet
Port 6003 wurde fÃ¼r die Protokolle tcp und udp geÃ¶ffnet.
Port 5769 wurde fÃ¼r das tcp Protokoll geÃ¶ffnet.
DRÃCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 155: Installer meldet das Firewall Port 6003 und 5769 geöffnet wurden

Um zu prüfen, ob die Ports 6003 und 5769 erfolgreich geöffnet wurden, könen Sie manuell überprufen, siehe Kapitel RCCMD FAQs.

Beachten Sie die Firewall Ausnahmen.

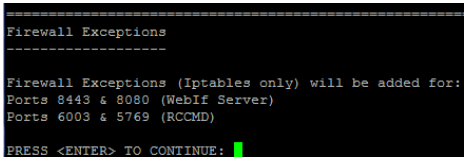
Firewall Exceptions
Firewall Exceptions (Iptables only) will be added for:
Ports 8443 & 8080 (WebIf Server)
Ports 6003 & 5769 (RCCMD)
PRESS <ENTER> TO CONTINUE:

Abb. 156: Firewall Ausnahmen

4.2.4 RCCMD WebInterface Konfiguration (ab Version 4.2.0.0)

Nach erfolgreicher Installation wird RCCMD automatisch gestartet und ist sofort bereit, Shutdown Kommandos von jedem RCCMD Server entgegen zu nehmen (Default-Einstellung).

Ab der RCCMD Version 4.2.0.0 verfügt RCCMD über ein eigenes Webinterface, dass den Remote Zugriff ermöglicht. Bitte beachten Sie, dass der Firewall Port 8443 TCP freigeschaltet sein muss. Geben Sie in einem Webbrowser Folgendes ein, um sich remote auf die vMA zu verbinden, auf der RCCMD installiert wurde:

https://IP-Adresse des RCCMD Rechners:8443

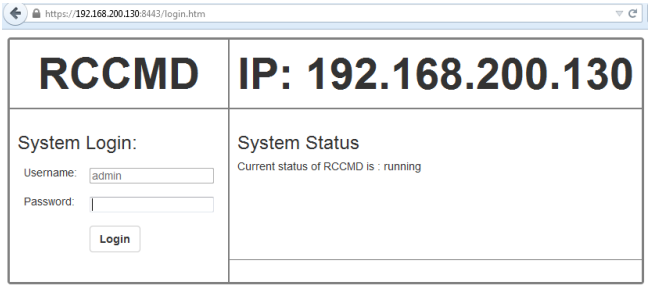

Abb. 157: RCCMD WebInterface – Remote Zugriff

Nun besteht die Möglichkeit, die Konfiguration bzw. Steuerung aus der Ferne auszuführen.

Im vCenter können Sie über den Tab „RCCMD Client“ ebenfalls RCCMD konfigurieren.

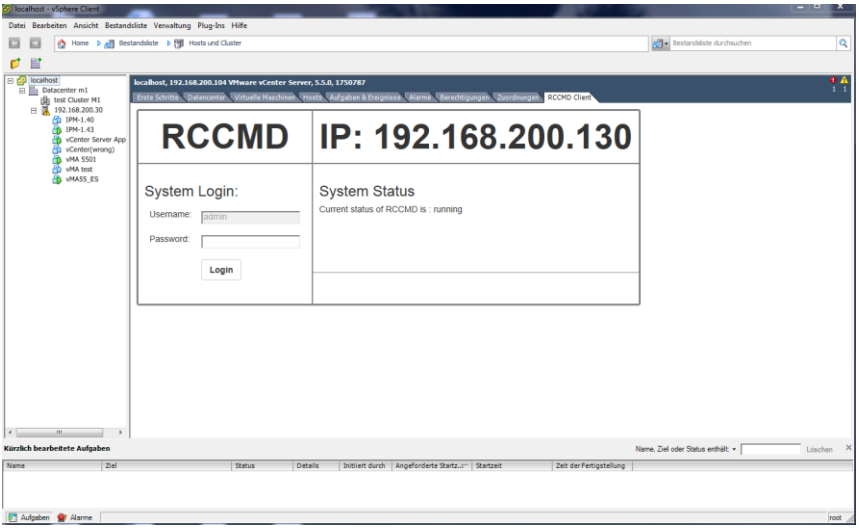

Abb. 158: RCCMD WebInterface – RCCMD im vCenter

Im Menü „**Connections**“ können Sie die IP-Adressen der berechtigten RCCMD Sender (CS121/UPSMAN) eintragen. Klicken Sie auf „Insert“, um die IP-Adresse des ersten Senders einzutragen. Klicken Sie auf „Remove“, wenn Sie die eingetragene IP-Adresse herausnehmen möchten. Klicken Sie auf „Edit“, wenn Sie die eingetragene IP-Adresse bearbeiten möchten.

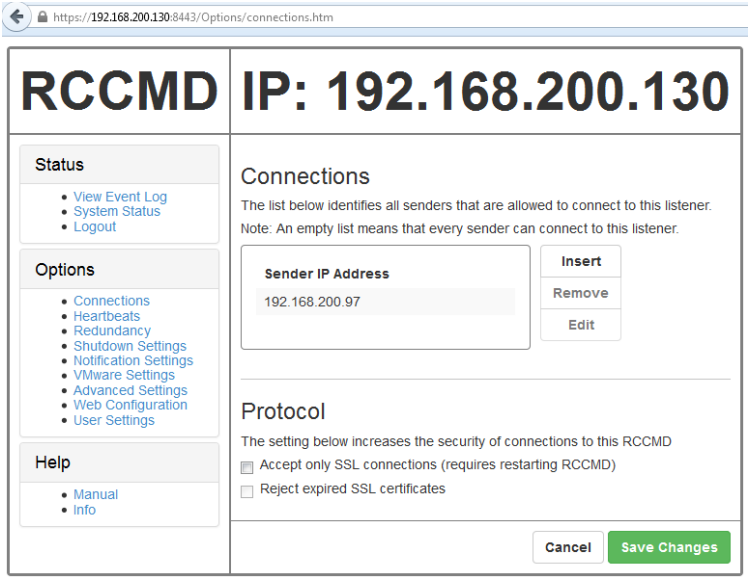

Abb. 159: RCCMD WebInterface – Connections

Achtung: **Wenn Sie hier keine Adresse eintragen, ist jeder Server in der Lage, einen Shutdown an diesen Client zu senden.**

Unter „**Protocols**“ kann definiert werden, ob RCCMD mit SSL Zertifikaten verwendet wird. Aktivieren Sie „Reject expired SSL certificates“, wenn Sie Verbindungen mit abgelaufenen SSL Zertifikaten ablehnen wollen. Weitere Informationen für RCCMD mit SSL finden Sie in Kapitel 6.6.1.

Klicken Sie vor Verlassen des „Connections“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Heartbeats**“ kann die Funktion „UPSMAN Alive Check“ aktiviert werden.

Dieser Check ist ein Signal, das an den CS121 oder UPSMAN via Port 5769 gesendet wird, um zu prüfen, ob der UPSMAN noch USV Daten hat. Wenn nicht, wird das Script File “Alive.Bat” ausgeführt, das eine entsprechende Nachricht als Pop-Up bringt.

Die Funktion “by the use CS121/UPSMAN Traps” ermöglicht UPSMAN/RCCMD/UNMS Meldungen, die den USV Status als Nachricht anzeigen. Wenn aktiviert, wird diese

Funktion eine lokale Nachricht bringen, wenn der USV Status des UPSMAN/RCCMD Servers sich verändert.

Die Funktion „by polling CS121/UPSMAN every x seconds“ ermöglicht die reine Signalabfrage, ohne das Empfangen von USV-Werten bzw. Nachrichten.

Die Polling Rate (Standard 1800 Sekunden) definiert den Interval der UPSMAN Abfrage, connection retries (Verbindungswiederholungen, Standard 5) bedeutet, das nach 5 erfolglosen Verbindungsversuchen ein Alarm ausgelöst wird.

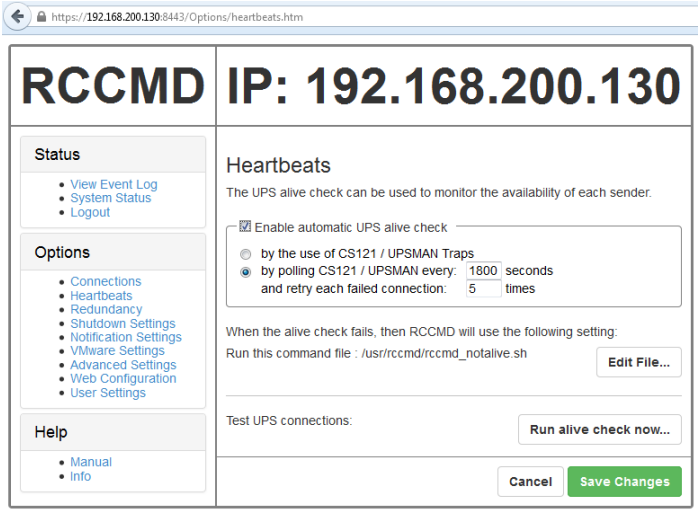

Abb. 160: RCCMD WebInterface – Heartbeats

Wenn Sie auf “Run alive check now…” klicken, wird das UPSMAN Alive Checking von der eingetragenen IP-Adresse gestartet (der Port 5769 wird getestet).

Klicken Sie vor Verlassen des „Heartbeats“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Redundancy**“ kann die Redundanz Management Funktion aktiviert werden. Der Redundanz Level definiert die Anzahl der redundanten Sender in der Redundanz Gruppe. Das bedeutet, dass bei einem Redunz Level von 1 beide RCCCMD Sender (CS121/UPSMAN) einen Shutdown gesendet haben müssen, bevor RCCMD seine Shutdown Sequenz startet.

Wenn RCCMD einen Shutdown unterdrückt, erhalten Sie eine Nachrichten Box aus der „Suppressed.bat“, die Sie verändern können, wenn Sie auf „Edit File...“ klicken.

Bitte beachten Sie, dass für das Zurücksetzen des Redundanz Alarms eine Event Konfiguration auf dem Sender (CS121/UPSMAN) erforderlich ist. Die Funktion „Send RCCMD cancle shutdown“ kann verwendet werden, um automatisch einen vorher abgesendeten Shutdown zu verwerfen. Wenn ein Shutdown unterdrückt wurde, wegen

der zu diesem Zeitpunkt noch vorhandenen Redundanz, das Problem aber zwischenzeitlich an der USV gelöst wurde, kann mittels einem „Send RCCMD cancel shutdown“ der Alarm zurückgesetzt werden. Durch diesen Befehl wird der RCCMD Client, der vorher das Shutdownsignal erhalten hat, aufgefordert, dieses wieder rückgängig zu machen.

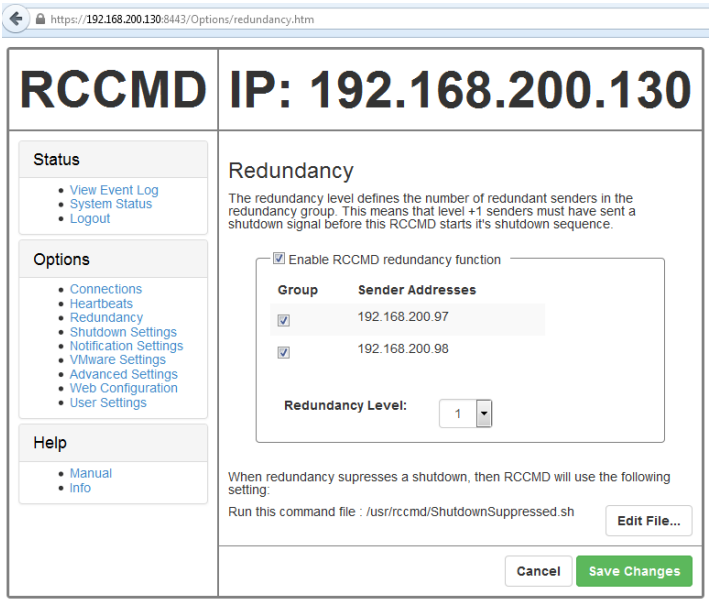

Abb. 161: RCCMD WebInterface – Redundancy

Schauen Sie bitte in das Kapitel 6.1 für ausführlichere Informationen zu RCCMD mit Redundanz.

Klicken Sie vor Verlassen des „Redundancy“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Shutdown Settings**“ können Sie die Shutdown Sequenz verändern bzw. erweitern. Als Standard wird die rccmd_shutdown.sh verwendet:

```
#!/bin/sh

# rccmd_shutdown.sh - This script is called by rccmd after receiving

# the "SHUTDOWN" command from the network.

RCCMD_DIR=/usr/rccmd

ESXI_HOST_SHUTDOWN=${RCCMD_DIR}/shutdown_ESXI.sh

FREE_ESXI_SHUTDOWN=${RCCMD_DIR}/shutdown_freeESXi.sh

${ESXI_HOST_SHUTDOWN}
```

IMPORTANT: Read instructions contained in shutdown_freeESXi.sh before use!

#${FREE_ESXI_SHUTDOWN}

exit $?

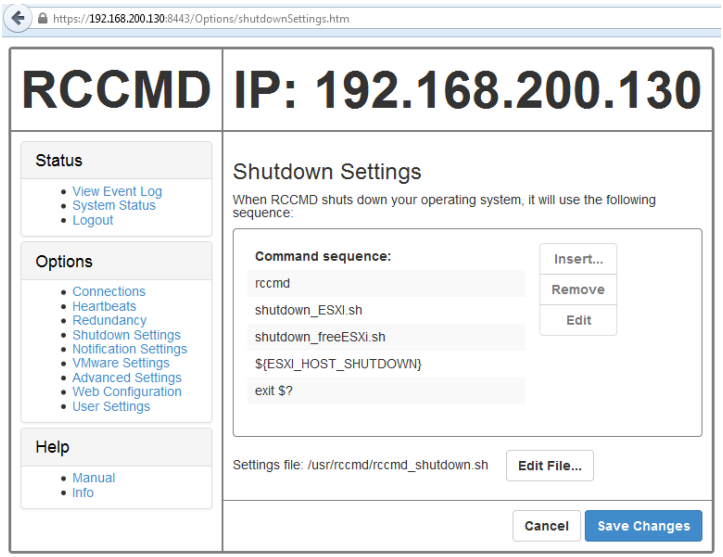

Abb. 162: RCCMD WebInterface – vMA Shutdown Settings

Achtung: **Wir empfehlen, die „Command sequence“ für den Shutdown einer vMA NICHT zu ändern! Die Features „Insert command...“ und „Edit File...“ machen nur auf anderen Betriebssystemen Sinn.**

Im Menü „**Notification Settings**“ können Sie die entsprechenden Standard Bat-Files für E-Mail, Message (Nachrichten) und Execute (auszuführende Kommandos) verändern bzw. erweitern, wenn Sie auf „Edit File...“ klicken.

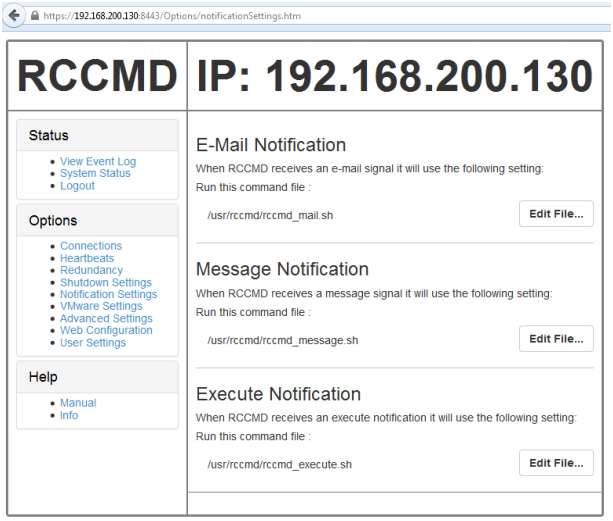

Abb. 163: RCCMD WebInterface – Notification Settings

Klicken Sie vor Verlassen des „Notification Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im VMware Settings Menü, wo Sie die Parameter/Features sehen können, die Sie während der Installation angegeben/ausgewählt haben, können hier nachträglich Änderungen vorgenommen werden.

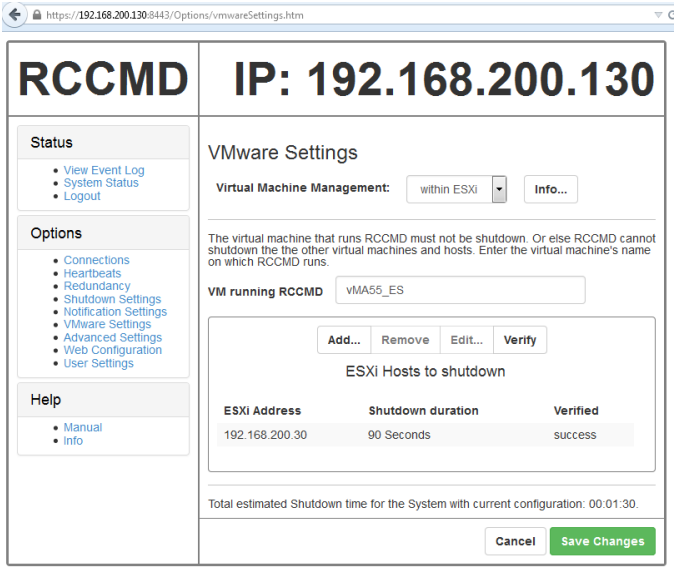

Abb. 164: RCCMD WebInterface – Remote Zugriff – VMware Settings

Wählen Sie **„Virtual Machine Management: within ESXi“**, um dem ESXi die Kontrolle über die virtuellen Maschinen während des Shutdowns zu geben.

Über den „Verify“ Button besteht die Möglichkeit, die Zugangsdaten und die Verbindung zum ESXi Host zu verifizieren.

Achtung: **Bitte beachten Sie, dass der Name der vMA im RCCMD Menu „VMware Settings“ identisch mit dem Namen der vMA im vSphere Client bzw. vCenter sein muss!**

Wenn Sie einen weiteren physikalischen Host hinzufügen möchten, können Sie das via „Add“ ausführen und die entsprechenden Parameter angeben.

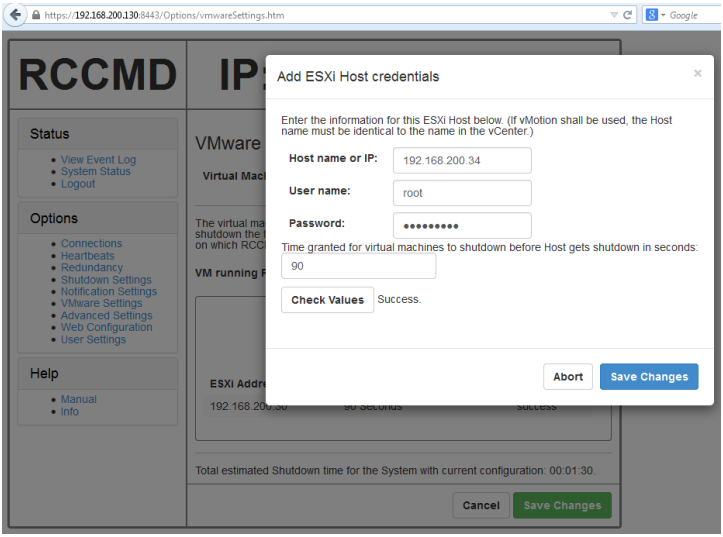

Abb. 165: RCCMD WebInterface – Remote Zugriff – VMware Settings – Add Host

4.2.4.1 RCCMD WebInterface mit vCenter

Nach der erfolgreichen Installation mit vCenter, ist es erforderlich, die Zugangsdaten der in rot aufgeführten ESXi Hosts über den „Edit“ Button anzugeben und diese über den „Verify“ Button zu verifizieren.

Achtung: **Bitte beachten Sie, dass der Name der vMA im RCCMD Menu „VMware Settings“ identisch mit dem Namen der vMA im vSphere Client bzw. vCenter sein muss!**

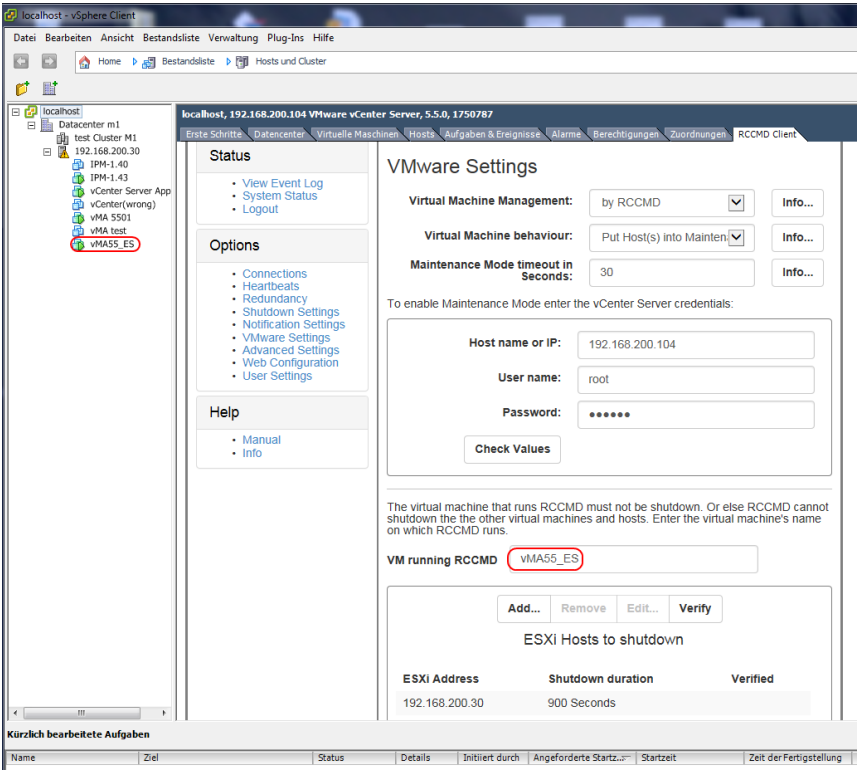

Abb. 166: RCCMD WebInterface – VMware Settings – vMA Name

Wählen Sie **„Virtual Machine Management: by RCCMD“**, wenn die Hosts von einem vCenter Server gesteuert werden. RCCMD muss für das Shutdown-Verhalten konfiguriert werden.

Die Auswahl **„Virtual Machine Behaviour: Shutdown Virtual Machines“** ist die sicherste Variante. In diesem Fall sendet RCCMD ein Shutdown Signal via VMware Tools zu den laufenden virtuellen Maschinen auf jeden Host. Die Reihenfolge, in der die virtuellen Maschinen heruntergefahren werden, ist nicht konfigurierbar.

Die Auswahl **„Virtual Machines Behaviour: Put Host(s) into Maintenance Mode“** kann versuchen, einen Host in den Maintenance Mode zu schalten und dadurch vMotion für die virtuellen Maschinen auszulösen. Wählen Sie diese Option nur, wenn DRS (Distributed Resources Scheduler) im voll automatisierten Modus konfiguriert ist und vMotion erfolgreich für jede virtuelle Maschine getestet wurde! Wenn das Schalten in Maintenance Mode fehlschlägt, dann werden die verbleibenden Hosts mit dem „Shutdown Virtual Machines Behaviour“ fortfahren. Um zu kalkulieren, wieviel Autonomie Zeit verbleibt, wenn das RCCMD Kommando initiiert wird, müssen die längste „Shutdown Duration“ (Dauer des Herunterfahrens) und der Maintenance Mode Timeout addiert werden.

Tragen Sie den Zeitpunkt ein, nach dem das Schalten in den Maintenance Mode abgebrochen wird. Wenn der Schaltvorgang in den Maintenance Mode in dieser Zeit nicht funktioniert, dann werden die verbleibenden Hosts mit dem „Shutdown Virtual Machines Behaviour“ fortfahren. Dies ist der letzte Versuch, die virtuellen Maschinen und die Hosts sauber herunterzufahren.

Sie können erneut die Zugangsdaten des vCenters mit dem Button „Check Values“ überprüfen.

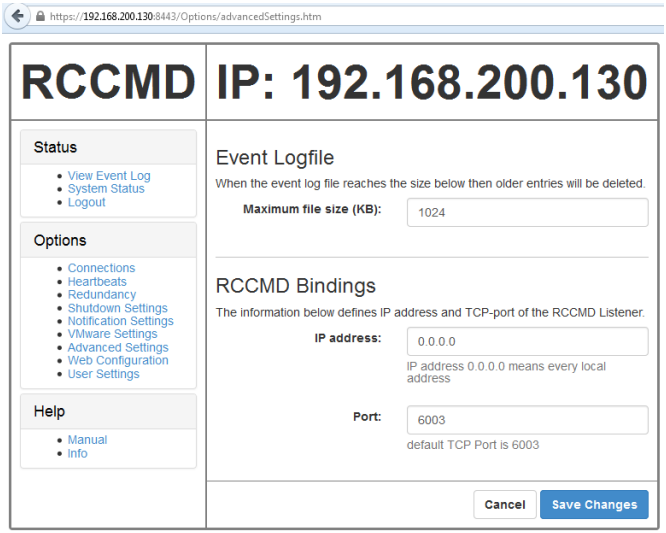

Abb. 167: RCCMD WebInterface – Advanced Settings

Im Menü „**Advanced Settings**“ können Sie die maximale Grösse des Event Logfiles definieren, bei der das Überschreiben älterer Einträge beginnt, die RCCMD Bindings für die IP-Adresse und den RCCMD Listener TCP Port.

Klicken Sie vor Verlassen des „Advanced Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Web Configuration**“ besteht die Möglichkeit, das HTTPS Protokoll zu deaktivieren, um nur mit dem HTTP Protokoll zu arbeiten. Ab der RCCMD Version 4.2.3.0 gibt es die Möglichkeit, die Standard Ports für HTTP bzw. HTTPS zu ändern und danach direkt den RCCMD WebIf neuzustarten.

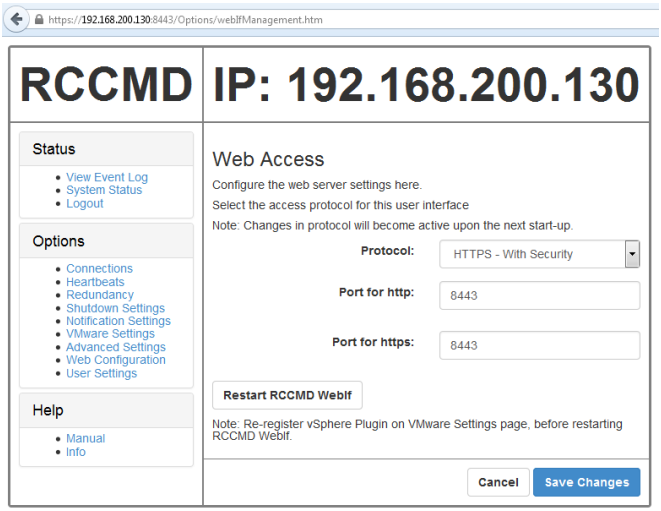

Abb. 168: RCCMD WebInterface – Web Access

Klicken Sie vor Verlassen des „Web Configuration“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern. Klicken Sie auf „Logout“, wenn Sie den Web Configurator nicht mehr benötigen.

Klicken Sie vor Verlassen des „Web Configuration“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**User Settings**“ können Sie das Standard Passwort für den Benutzer „admin“ wie gewünscht ändern und den RCCMD WebIf neustarten.

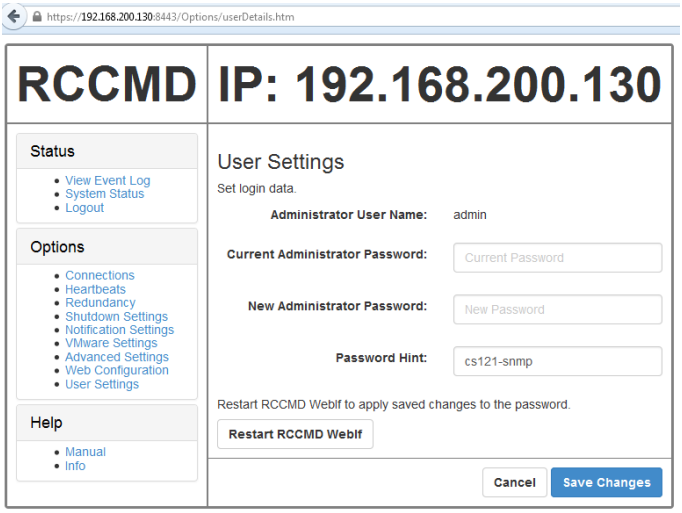

Abb. 169: RCCMD WebInterface – User Settings

Klicken Sie vor Verlassen des „User Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern. Klicken Sie auf „Logout“, wenn Sie den Web Configurator nicht mehr benötigen.

Im Menü „**Status, View Event Log**“ können Sie die Protokollierung der bisherigen Ereignisse einsehen.

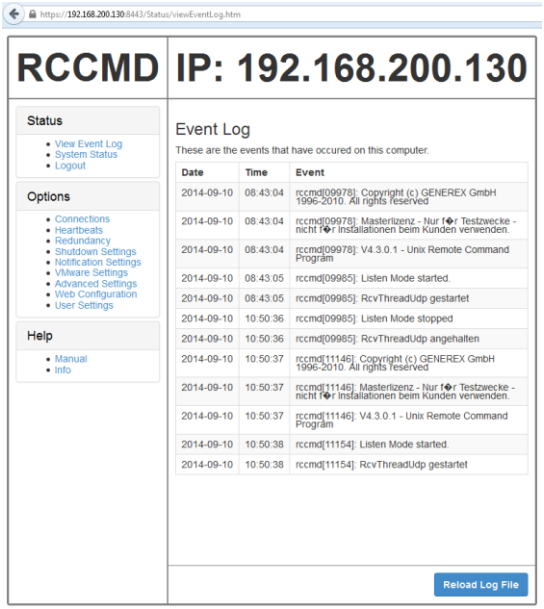
https://192.168.200.130:8443/Status/viewEventLog.htm
RCCMD
IP: 192.168.200.130
Status
View Event Log
System Status
Logout
Options
Connections
Heartbeats
Redundancy
Shutdown Settings
Notification Settings
VMware Settings
Advanced Settings
Web Configuration
User Settings
Help
Manual
Info
Event Log
These are the events that have occured on this computer.
Date
Time
Event
2014-09-10 08:43:04 rccmd[09978]: Copyright (c) GENEREX GmbH 1996-2010. All rights reserved
2014-09-10 08:43:04 rccmd[09978]: Masterlizenz - Nur f	r Testzwecke - nicht f	r Installationen beim Kunden verwenden.
2014-09-10 08:43:04 rccmd[09978]: V4.3.0.1 - Unix Remote Command Program
2014-09-10 08:43:05 rccmd[09985]: Listen Mode started.
2014-09-10 08:43:05 rccmd[09985]: RcvThreadUdp gestartet
2014-09-10 10:50:36 rccmd[09985]: Listen Mode stopped
2014-09-10 10:50:36 rccmd[09985]: RcvThreadUdp angehalten
2014-09-10 10:50:37 rccmd[11146]: Copyright (c) GENEREX GmbH 1996-2010. All rights reserved
2014-09-10 10:50:37 rccmd[11146]: Masterlizenz - Nur f	r Testzwecke - nicht f	r Installationen beim Kunden verwenden.
2014-09-10 10:50:37 rccmd[11146]: V4.3.0.1 - Unix Remote Command Program
2014-09-10 10:50:38 rccmd[11154]: Listen Mode started.
2014-09-10 10:50:38 rccmd[11154]: RcvThreadUdp gestartet
Reload Log File

Abb. 170: RCCMD WebInterface – Event Log

Im Menü „**Status, System Status**“ können Sie den aktuellen Status von RCCMD überprüfen, den Status updaten und den RCCMD Dienst neustarten bzw. stoppen und starten.

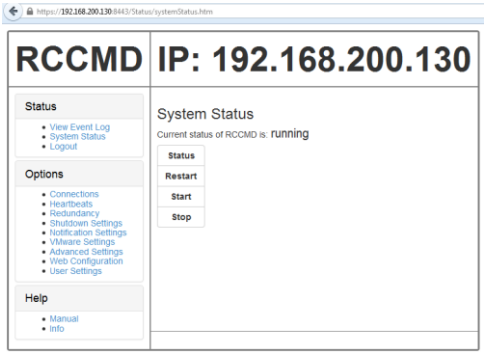

Abb. 171: RCCMD WebInterface – System Status

Im Menü „**Help**“ können Sie das RCCMD Benutzerhandbuch zu Ihrer Unterstützung aufrufen, können dem Link auf www.generex.de folgen und die Installer Version via „Info“ anzeigen.

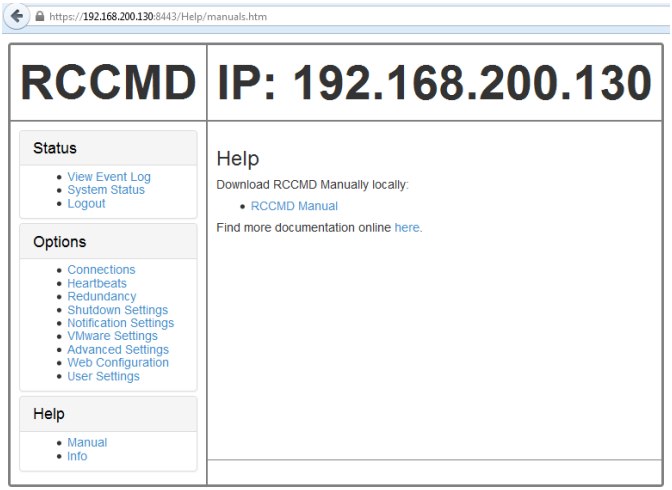

Abb. 172: RCCMD WebInterface – Help

Achtung: **Bitte beachten Sie, dass die vMA nach einem Shutdown manuell gestartet werden muss!**

4.2.5 RCCMD Installation auf der vMA 6 (ab RCCMD V 4.3.0.2)

Verwenden Sie ihre RCCMD Client-Lizenznummer, und laden Sie sich von der Website des USV Herstellers oder von www.generex.de den RCCMD client für VMware ESXi herunter. RCCMD wird im Download als sogenannte „TAR“ Datei geliefert. Kopieren Sie die Datei rccmdinst.tar mit Hilfe des SCP Clients (SFTP) auf die vMA. Einen SFTP Client kann als Freeware aus dem Internet verwendet werden, z. B. Filezilla oder ein ähnliches Tool kann die Funktion der Überrtragung des RCCMD Pakets auf das Zielsystem ausführen.

- Loggen Sie sich auf der vMA ein. Für das Einloggen auf der vMA wird ein Terminalprogramm benötigt, z. B. Putty oder einer anderen Terminalsoftware.
- Erstellen Sie z. B. mit „mkdir“ ein temporäres Verzeichnis z. B. mit dem Namen „RCCMD“, wohin Sie dann die TAR Datei hineinkopieren.
- Entpacken Sie die tar-Datei mit dem Befehl: „`tar -xvf rccmdinst.tar`“

Es entstehen folgende Dateien nach dem Entpackvorgang:

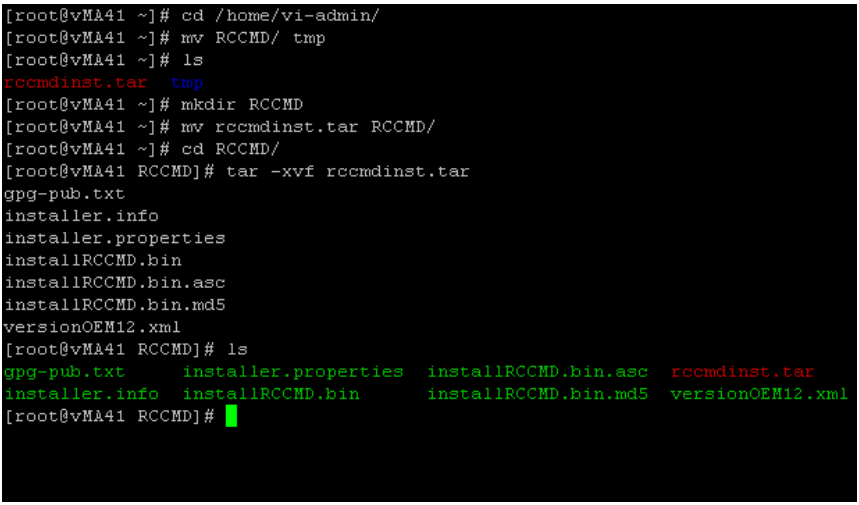

Abb. 173: Installationsvorbereitung

Sie sollten als „root“ eingeloggt sein und damit Administratorrechte besitzen.

Starten Sie die Installation mit dem Aufruf: `./installRCCMD.bin`

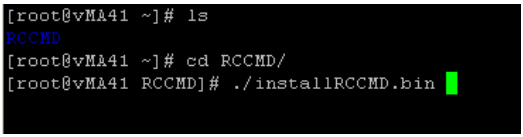

Abb. 174: Ausführung der Binärdatei installRCCMD.bin und Beginn des Installationsskriptes

Alternativ können Sie auch mit dem „Sudo-Befehl“ als vi-admin installieren:

```
sudo ./installRCCMD.bin
```

Wählen Sie die Sprache aus, und drücken Sie die Eingabetaste.

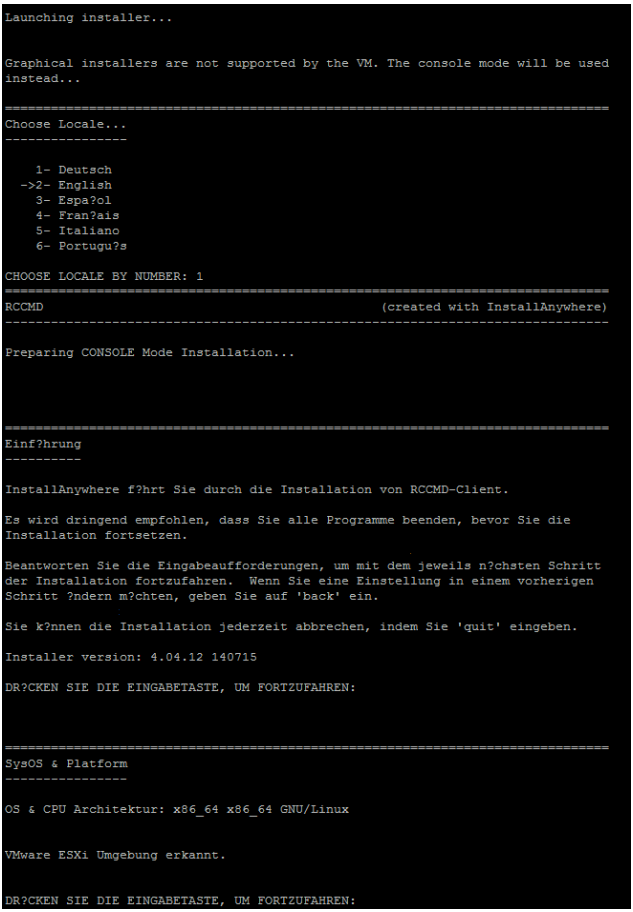
Launching installer...
Graphical installers are not supported by the VM. The console mode will be used instead...
Choose Locale...
1- Deutsch
->2- English
3- Espa?ol
4- Fran?ais
5- Italiano
6- Portugu?s
CHOOSE LOCALE BY NUMBER: 1
RCCMD
(created with InstallAnywhere)
Preparing CONSOLE Mode Installation...
Einf?hrung
InstallAnywhere f?hrt Sie durch die Installation von RCCMD-Client.
Es wird dringend empfohlen, dass Sie alle Programme beenden, bevor Sie die Installation fortsetzen.
Beantworten Sie die Eingabeaufforderungen, um mit dem jeweils n?chsten Schritt der Installation fortzufahren. Wenn Sie eine Einstellung in einem vorherigen Schritt ?ndern m?chten, geben Sie auf 'back' ein.
Sie k?nnen die Installation jederzeit abbrechen, indem Sie 'quit' eingeben.
Installer version: 4.04.12 140715
DR?CKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:
SysOS & Platform
OS & CPU Architektur: x86_64 x86_64 GNU/Linux
VMware ESXi Umgebung erkannt.
DR?CKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 175: Sprachauswahl und Beginn der Installation - die Meldung „Recognized VMware ESXi environment“ zeigt an, dass die richtige Hardware erkannt wurde

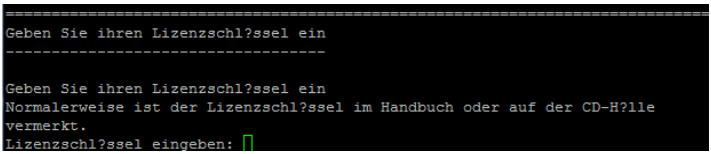
Geben Sie ihren Lizenzschl?ssel ein
Geben Sie ihren Lizenzschl?ssel ein
Normalerweise ist der Lizenzschl?ssel im Handbuch oder auf der CD-H?lle vermerkt.
Lizenzschl?ssel eingeben:

Abb. 176: Lizenz Eingabe

Geben Sie den RCCMD Lizenzschlüssel ein. Wählen Sie die Produkt Features, die Sie installieren möchten.

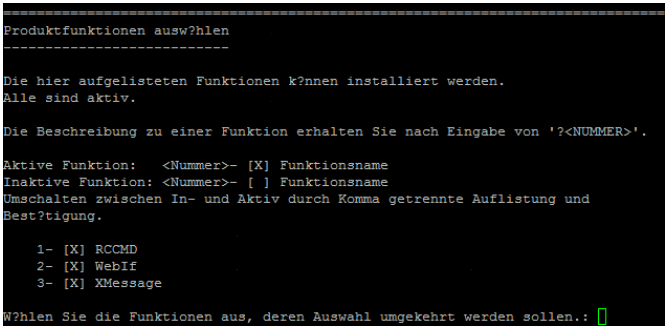
Produktfunktionen ausw?hlen
Die hier aufgelisteten Funktionen k?nnen installiert werden.
Alle sind aktiv.
Die Beschreibung zu einer Funktion erhalten Sie nach Eingabe von '?<NUMMER>'.
Aktive Funktion: <Nummer>- [X] Funktionsname
Inaktive Funktion: <Nummer>- [ ] Funktionsname
Umschalten zwischen In- und Aktiv durch Komma getrennte Auflistung und
Best?tigung.
1- [X] RCCMD
2- [X] WebIf
3- [X] XMessage
W?hlen Sie die Funktionen aus, deren Auswahl umgekehrt werden sollen.:

Abb. 177: Produkt Feature Auswahl

4.2.5.1 RCCMD Installation ohne vCenter

Danach geben Sie bitte an, ob sich ein vCenter in Ihrer VMware Umgebung befindet und den Hostnamen oder die IP-Adresse des ESXi Servers.

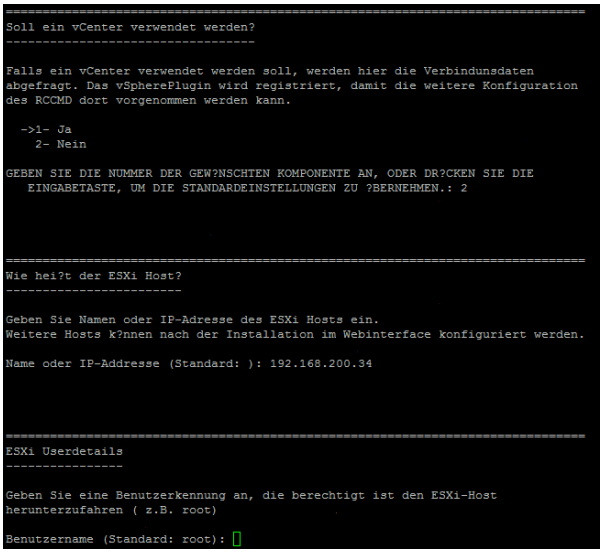
Soll ein vCenter verwendet werden?
Falls ein vCenter verwendet werden soll, werden hier die Verbindunsdaten
abgefragt. Das vSpherePlugin wird registriert, damit die weitere Konfiguration
des RCCMD dort vorgenommen werden kann.
->1- Ja
2- Nein
GEBEN SIE DIE NUMMER DER GEW?NSCHTEN KOMPONENTE AN, ODER DR?CKEN SIE DIE
EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ?BERNEHMEN.: 2
Wie hei?t der ESXi Host?
Geben Sie Namen oder IP-Adresse des ESXi Hosts ein.
Weitere Hosts k?nnen nach der Installation im Webinterface konfiguriert werden.
Name oder IP-Addresse (Standard:): 192.168.200.34
ESXi Userdetails
Geben Sie eine Benutzerkennung an, die berechtigt ist den ESXi-Host
herunterzufahren (z.B. root)
Benutzername (Standard: root):

Abb. 178: Interaktive Eingaben – vCenter, ESXi Server Hostname oder IP-Adresse

Geben Sie die Zeit an, die für den Shutdown der virtuellen Maschinen benötigt wird und weitere Details.

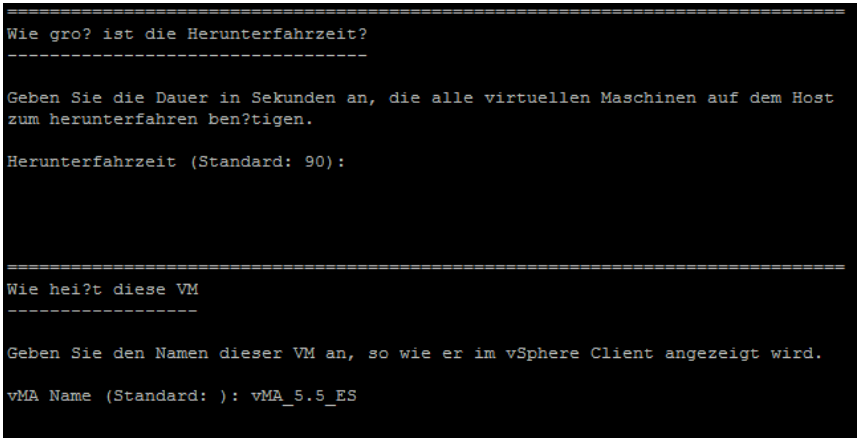
Wie gro? ist die Herunterfahrzeit?
Geben Sie die Dauer in Sekunden an, die alle virtuellen Maschinen auf dem Host zum herunterfahren ben?tigen.
Herunterfahrzeit (Standard: 90):
Wie hei?t diese VM
Geben Sie den Namen dieser VM an, so wie er im vSphere Client angezeigt wird.
vMA Name (Standard:): vMA_5.5_ES

Abb. 179: Interaktive Eingaben – Herunterfahrzeit, vMA Name

4.2.5.2 RCCMD Installation mit vCenter 6 (ab RCCMD V 4.3.0.2)

Geben Sie die Zugangsdaten für das vCenter ein.

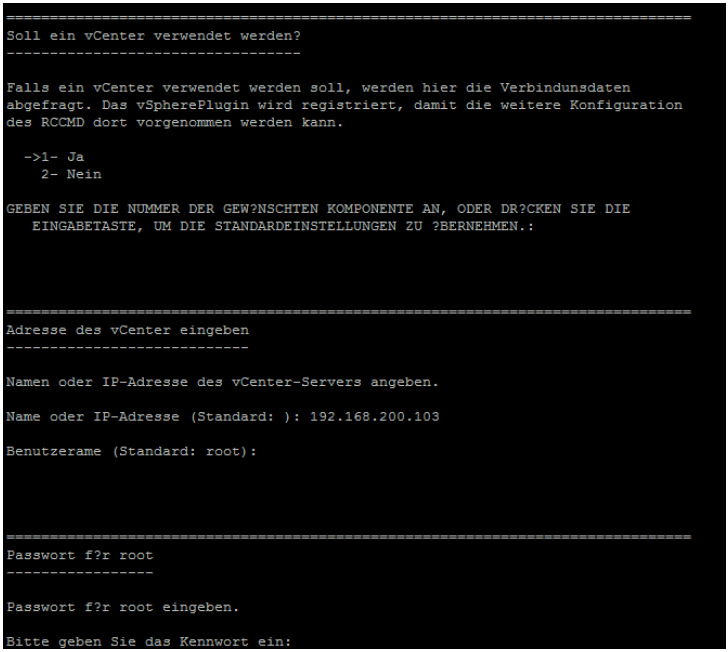
Soll ein vCenter verwendet werden?
Falls ein vCenter verwendet werden soll, werden hier die Verbindunsdaten abgefragt. Das vSpherePlugin wird registriert, damit die weitere Konfiguration des RCCMD dort vorgenommen werden kann.
->1- Ja
2- Nein
GEBEN SIE DIE NUMMER DER GEW?NSCHTEN KOMPONENTE AN, ODER DR?CKEN SIE DIE EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ?BERNEHMEN.:
Adresse des vCenter eingeben
Namen oder IP-Adresse des vCenter-Servers angeben.
Name oder IP-Adresse (Standard:): 192.168.200.103
Benutzerame (Standard: root):
Passwort f?r root
Passwort f?r root eingeben.
Bitte geben Sie das Kennwort ein:

Abb. 180: Interaktive Eingaben – vCenter Zugangsdaten

Es folgt die Installationsübersicht.

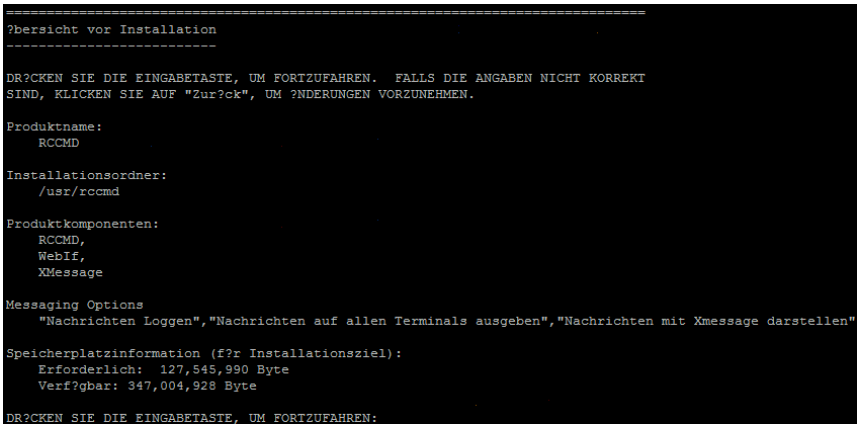

Abb. 181: Interaktive Eingaben – Installationsübersicht

Wählen Sie ein Protokoll und einen entsprechenden Port aus.

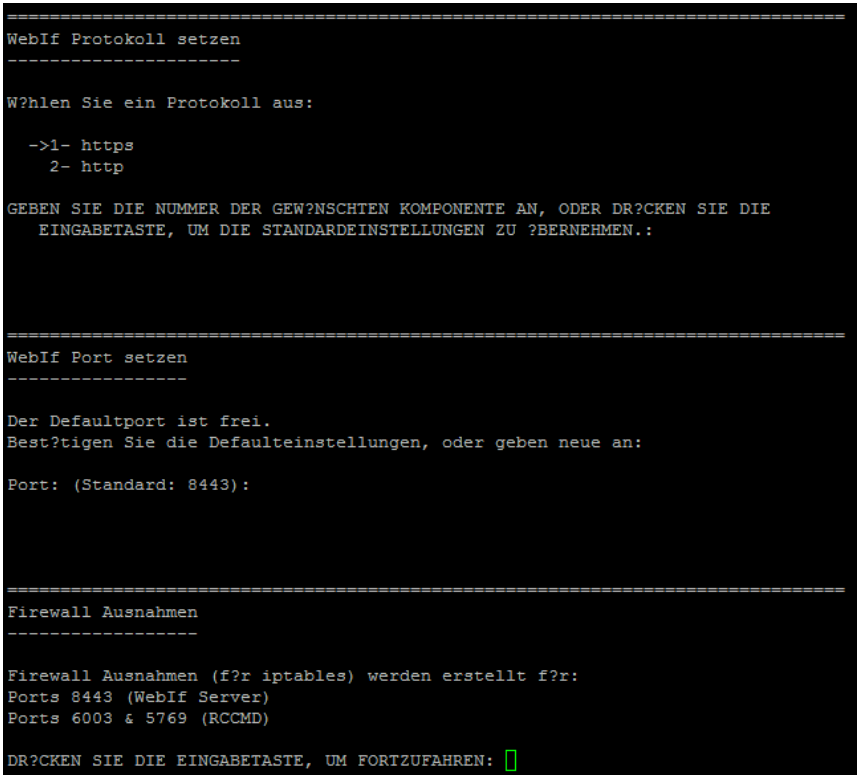
WebIf Protokoll setzen
W?hlen Sie ein Protokoll aus:
->1- https
2- http
GEBEN SIE DIE NUMMER DER GEW?NSCHTEN KOMPONENTE AN, ODER DR?CKEN SIE DIE
EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ?BERNEHMEN.:
WebIf Port setzen
Der Defaultport ist frei.
Best?tigen Sie die Defaulteinstellungen, oder geben neue an:
Port: (Standard: 8443):
Firewall Ausnahmen
Firewall Ausnahmen (f?r iptables) werden erstellt f?r:
Ports 8443 (WebIf Server)
Ports 6003 & 5769 (RCCMD)
DR?CKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 182: Interaktive Eingaben – Portauswahl, Firewall Ausnahmen

```
================================================================================
Passwort eingeben
-----------------

Setzen Sie ein Passwort f?r das RCCMD Webinterface. Wenn kein Passwort gesetzt
wird, verbleibt das standard Passwort bei "cs121-snmp"!

Passwort::



================================================================================
Passworthinweis eingeben.
-------------------------

Passworthinweis eingeben.

Passworthinweis (Standard: ):




================================================================================
RCCMD jetzt starten?
--------------------

Es wird empfohlen den RCCMD das erste Mal nach Konfiguration durch das WebIf zu
starten.
Wenn Sie den RCCMD manuell starten wollen, rufen Sie bitte "rccmdctl start"
auf.

Soll RCCMD jetzt direkt gestartet werden?

  ->1- Ja
    2- Nein

GEBEN SIE DIE NUMMER DER GEW?NSCHTEN KOMPONENTE AN, ODER DR?CKEN SIE DIE
   EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ?BERNEHMEN:



================================================================================
Installation abgeschlossen
---------------------------

Herzlichen Gl?ckwunsch. RCCMD-Client wurde erfolgreich im folgenden Verzeichnis
installiert:

     /usr/rccmd

DR?CKEN SIE DIE EINGABETASTE, UM DEN INSTALLER ZU BEENDEN:
```

Abb. 183: Interaktive Eingaben – Passworteingabe, Installationsabschluss

4.2.6 RCCMD WebInterface Konfiguration auf ESXi 6.x (ab RCCMD V 4.3.0.2)

Nach erfolgreicher Installation wird RCCMD automatisch gestartet und ist sofort bereit, Shutdown Kommandos von jedem RCCMD Server entgegen zu nehmen (Default-Einstellung).

Ab der RCCMD Version 4.2.0.0 verfügt RCCMD über ein eigenes Webinterface, dass den Remote Zugriff ermöglicht. Bitte beachten Sie, dass der Firewall Port 8443 TCP freigeschaltet sein muss. Geben Sie in einem Webbrowser Folgendes ein, um sich remote auf die vMA zu verbinden, auf der RCCMD installiert wurde:

https://IP-Adresse des RCCMD Rechners:8443

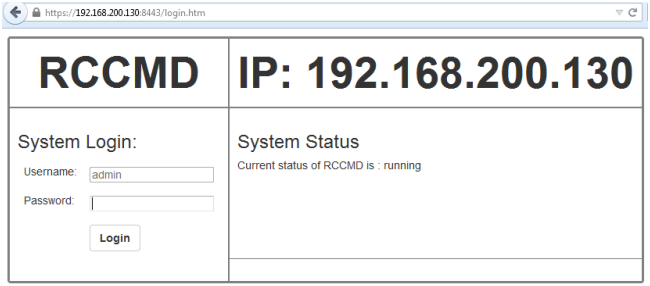

Abb. 184: RCCMD WebInterface – Remote Zugriff

Nun besteht die Möglichkeit, die Konfiguration bzw. Steuerung aus der Ferne auszuführen.

Im Menü „**Connections**“ können Sie die IP-Adressen der berechtigten RCCMD Sender (CS121/UPSMAN) eintragen. Klicken Sie auf „Insert“, um die IP-Adresse des ersten Senders einzutragen. Klicken Sie auf „Remove“, wenn Sie die eingetragene IP-Adresse herausnehmen möchten. Klicken Sie auf „Edit“, wenn Sie die eingetragene IP-Adresse bearbeiten möchten.

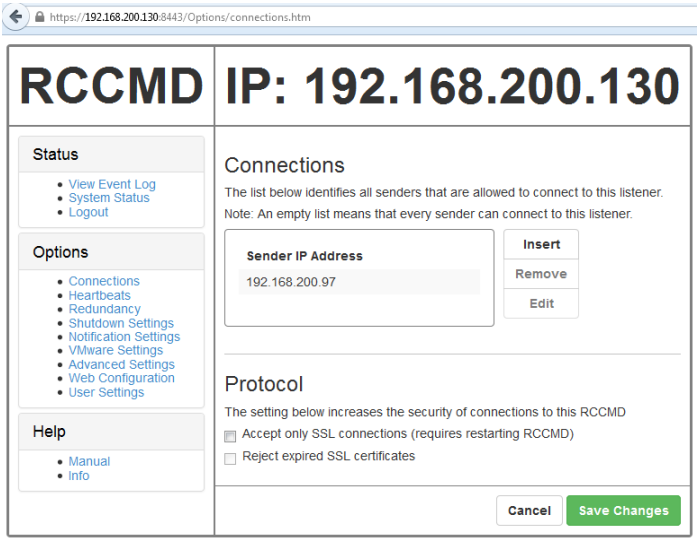

Abb. 185: RCCMD WebInterface – Connections

Achtung: **Wenn Sie hier keine Adresse eintragen, ist jeder Server in der Lage, einen Shutdown an diesen Client zu senden.**

Unter „**Protocols**“ kann definiert werden, ob RCCMD mit SSL Zertifikaten verwendet wird. Aktivieren Sie „Reject expired SSL certificates“, wenn Sie Verbindungen mit abgelaufenen SSL Zertifikaten ablehnen wollen. Weitere Informationen für RCCMD mit SSL finden Sie in Kapitel 6.6.1.

Klicken Sie vor Verlassen des „Connections“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Heartbeats**“ kann die Funktion „UPSMAN Alive Check“ aktiviert werden.

Dieser Check ist ein Signal, das an den CS121 oder UPSMAN via Port 5769 gesendet wird, um zu prüfen, ob der UPSMAN noch USV Daten hat. Wenn nicht, wird das Script File “Alive.Bat” ausgeführt, das eine entsprechende Nachricht als Pop-Up bringt.

Die Funktion “by the use CS121/UPSMAN Traps” ermöglicht UPSMAN/RCCMD/UNMS Meldungen, die den USV Status als Nachricht anzeigen. Wenn aktiviert, wird diese Funktion eine lokale Nachricht bringen, wenn der USV Status des UPSMAN/RCCMD Servers sich verändert.

Die Funktion „by polling CS121/UPSMAN every x seconds“ ermöglicht die reine Signalabfrage, ohne das Empfangen von USV-Werten bzw. Nachrichten.

Die Polling Rate (Standard 1800 Sekunden) definiert den Interval der UPSMAN Abfrage, connection retries (Verbindungswiederholungen, Standard 5) bedeutet, das nach 5 erfolglosen Verbindungsversuchen ein Alarm ausgelöst wird.

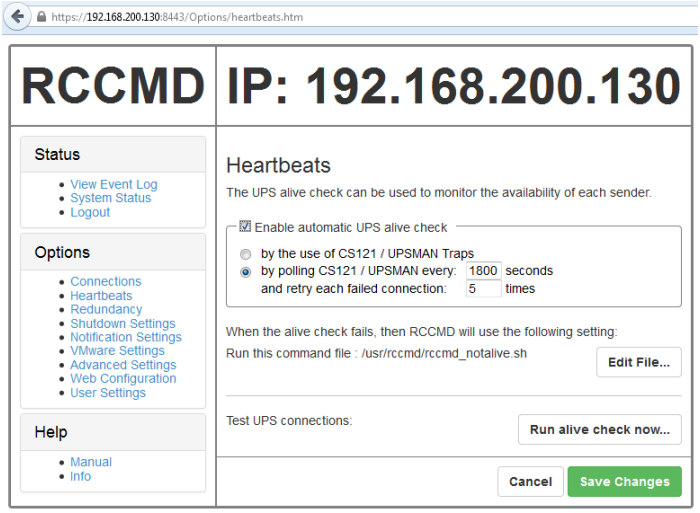

Abb. 186: RCCMD WebInterface – Heartbeats

Wenn Sie auf “Run alive check now…” klicken, wird das UPSMAN Alive Checking von der eingetragenen IP-Adresse gestartet (der Port 5769 wird getestet).

Klicken Sie vor Verlassen des „Heartbeats“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Redundancy**“ kann die Redundanz Management Funktion aktiviert werden. Der Redundanz Level definiert die Anzahl der redundanten Sender in der Redundanz Gruppe. Das bedeutet, dass bei einem Redunz Level von 1 beide RCCCMD Sender (CS121/UPSMAN) einen Shutdown gesendet haben müssen, bevor RCCMD seine Shutdown Sequenz startet.

Wenn RCCMD einen Shutdown unterdrückt, erhalten Sie eine Nachrichten Box aus der „Suppressed.bat“, die Sie verändern können, wenn Sie auf „Edit File...“ klicken.

Bitte beachten Sie, dass für das Zurücksetzen des Redundanz Alarms eine Event Konfiguration auf dem Sender (CS121/UPSMAN) erforderlich ist. Die Funktion „Send RCCMD cancle shutdown“ kann verwendet werden, um automatisch einen vorher abgesendeten Shutdown zu verwerfen. Wenn ein Shutdown unterdrückt wurde, wegen der zu diesem Zeitpunkt noch vorhandenen Redundanz, das Problem aber zwischenzeitlich an der USV gelöst wurde, kann mittels einem „Send RCCMD cancel shutdown“ der Alarm zurückgesetzt werden. Durch diesen Befehl wird der RCCMD Client, der vorher das Shutdownsignal erhalten hat, aufgefordert, dieses wieder rückgängig zu machen.

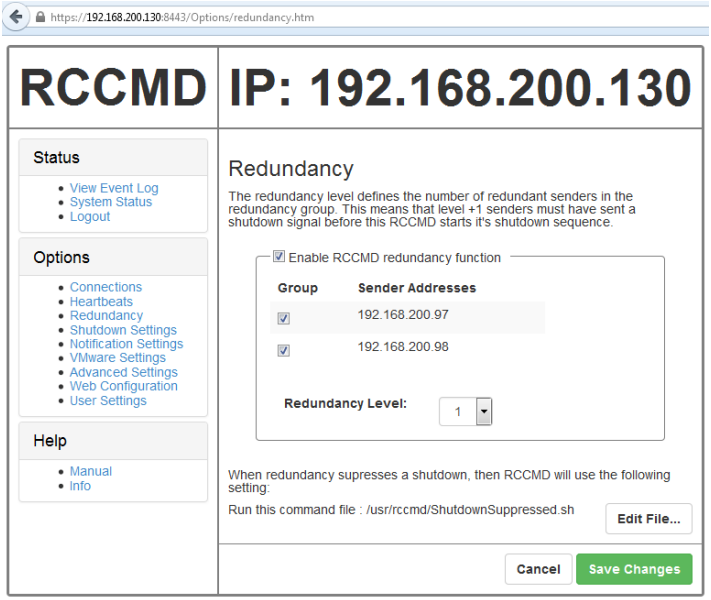

Abb. 187: RCCMD WebInterface – Redundancy

Schauen Sie bitte in das Kapitel 6.1 für ausführlichere Informationen zu RCCMD mit Redundanz.

Klicken Sie vor Verlassen des „Redundancy“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Shutdown Settings**“ können Sie die Shutdown Sequenz verändern bzw. erweitern. Als Standard wird die rccmd_shutdown.sh verwendet:

#!/bin/sh

rccmd_shutdown.sh - This script is called by rccmd after receiving

the "SHUTDOWN" command from the network.

RCCMD_DIR=/usr/rccmd

ESXI_HOST_SHUTDOWN=${RCCMD_DIR}/shutdown_ESXI.sh

FREE_ESXI_SHUTDOWN=${RCCMD_DIR}/shutdown_freeESXi.sh

${ESXI_HOST_SHUTDOWN}

IMPORTANT: Read instructions contained in shutdown_freeESXi.sh before use!

#${FREE_ESXI_SHUTDOWN}

exit $?

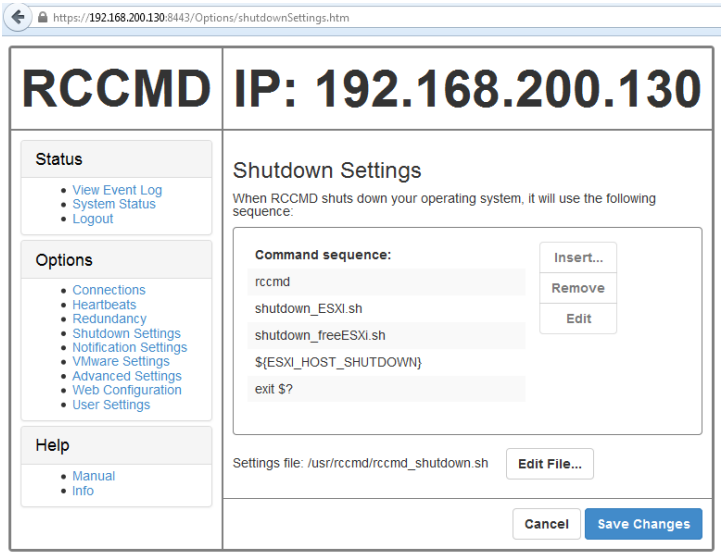

Abb. 188: RCCMD WebInterface – vMA Shutdown Settings

Achtung: **Wir empfehlen, die „Command sequence“ für den Shutdown einer vMA NICHT zu ändern! Die Features „Insert command...“ und „Edit File...“ machen nur auf anderen Betriebssystemen Sinn.**

Im Menü „**Notification Settings**“ können Sie die entsprechenden Standard Bat-Files für E-Mail, Message (Nachrichten) und Execute (auszuführende Kommandos) verändern bzw. erweitern, wenn Sie auf „Edit File...“ klicken.

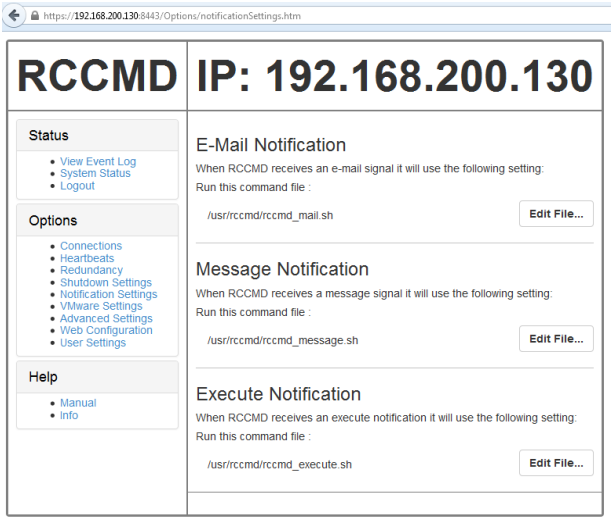

Abb. 189: RCCMD WebInterface – Notification Settings

Klicken Sie vor Verlassen des „Notification Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im VMware Settings Menü, wo Sie die Parameter/Features sehen können, die Sie während der Installation angegeben/ausgewählt haben, können hier nachträglich Änderungen vorgenommen werden.

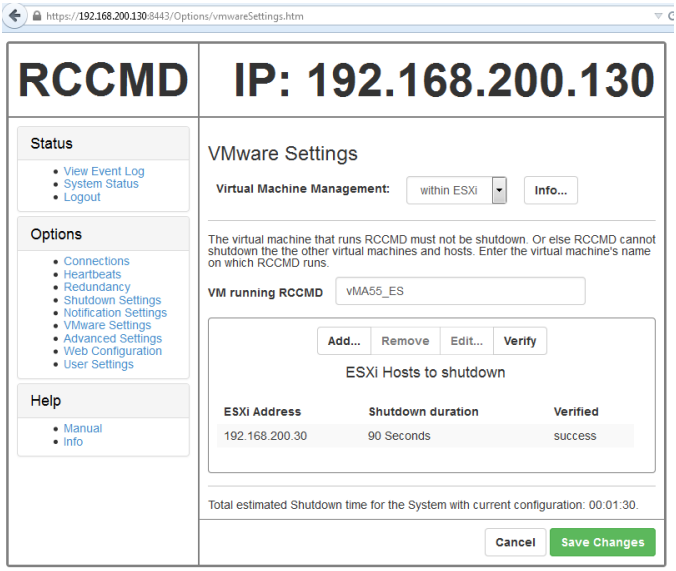

Abb. 190: RCCMD WebInterface – Remote Zugriff – VMware Settings

Wählen Sie **„Virtual Machine Management: within ESXi“**, um dem ESXi die Kontrolle über die virtuellen Maschinen während des Shutdowns zu geben.

Über den „Verify“ Button besteht die Möglichkeit, die Zugangsdaten und die Verbindung zum ESXi Host zu verifizieren.

Achtung: **Bitte beachten Sie, dass der Name der vMA im RCCMD Menu „VMware Settings“ identisch mit dem Namen der vMA im vSphere Client bzw. vCenter sein muss!**

Wenn Sie einen weiteren physikalischen Host hinzufügen möchten, können Sie das via „Add“ ausführen und die entsprechenden Parameter angeben.

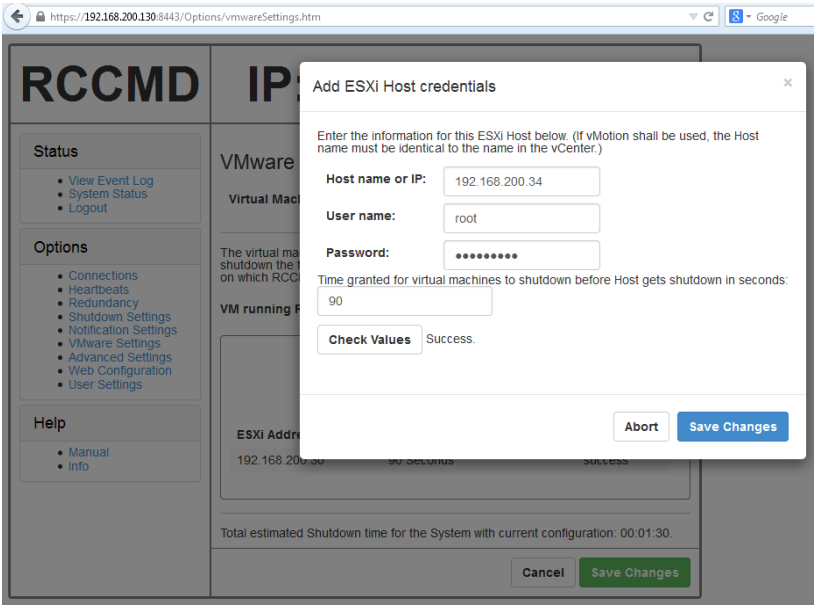

Abb. 191: RCCMD WebInterface – Remote Zugriff – VMware Settings – Add Host

4.2.6.1 RCCMD WebInterface mit vCenter 6 (ab RCCMD V 4.3.0.2)

Nach der erfolgreichen Installation mit vCenter, ist es erforderlich, die Zugangsdaten der in rot aufgeführten ESXi Hosts über den „Edit“ Button anzugeben und diese über den „Verify“ Button zu verifizieren.

Achtung:

Bitte beachten Sie, dass der Name der vMA im RCCMD Menu „VMware Settings“ identisch mit dem Namen der vMA im vSphere Client bzw. vCenter sein muss!

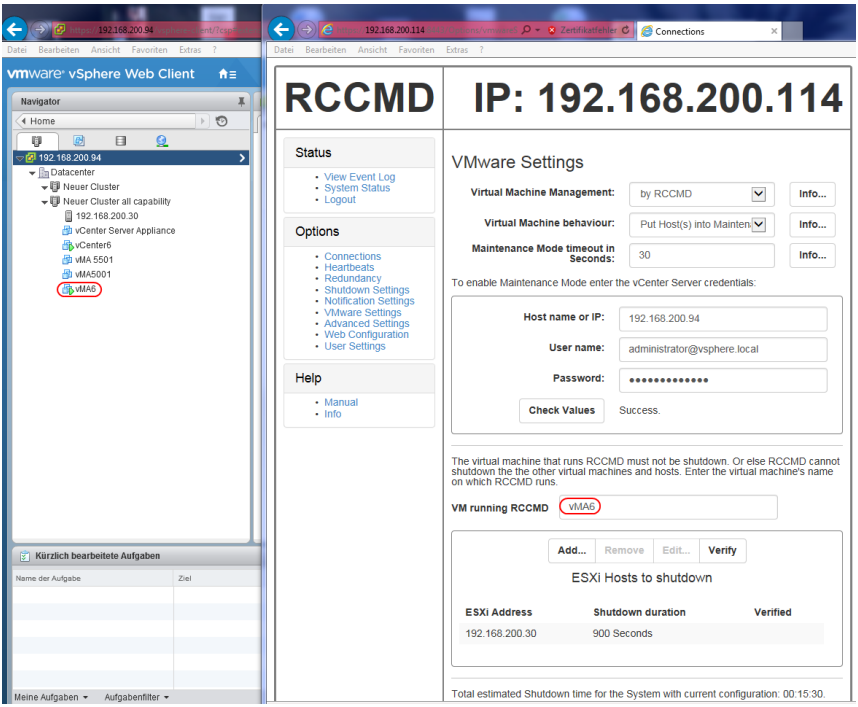

Abb. 192: vSphere Web Client, RCCMD WebInterface – VMware Settings – vMA Name

Wählen Sie **„Virtual Machine Management: by RCCMD“**, wenn die Hosts von einem vCenter Server gesteuert werden. RCCMD muss für das Shutdown-Verhalten konfiguriert werden.

Die Auswahl **„Virtual Machine Behaviour: Shutdown Virtual Machines“** ist die sicherste Variante. In diesem Fall sendet RCCMD ein Shutdown Signal via VMware Tools zu den laufenden virtuellen Maschinen auf jeden Host. Die Reihenfolge, in der die virtuellen Maschinen heruntergefahren werden, ist nicht konfigurierbar.

Die Auswahl **„Virtual Machines Behaviour: Put Host(s) into Maintenance Mode“** kann versuchen, einen Host in den Maintenance Mode zu schalten und dadurch vMotion für die virtuellen Maschinen auszulösen. Wählen Sie diese Option nur, wenn DRS (Distributed Resources Scheduler) im voll automatisierten Modus konfiguriert ist und vMotion erfolgreich für jede virtuelle Maschine getestet wurde! Wenn das Schalten in Maintenance Mode fehlschlägt, dann werden die verbleibenden Hosts mit dem „Shutdown Virtual Machines Behaviour“ fortfahren. Um zu kalkulieren, wieviel Autonomie Zeit verbleibt, wenn das RCCMD Kommando initiiert wird, müssen die längste „Shutdown Duration“ (Dauer des Herunterfahrens) und der Maintenance Mode Timeout addiert werden.

Tragen Sie den Zeitpunkt ein, nach dem das Schalten in den Maintenance Mode abgebrochen wird. Wenn der Schaltvorgang in den Maintenance Mode in dieser Zeit nicht

funktioniert, dann werden die verbleibenden Hosts mit dem „Shutdown Virtual Machines Behaviour“ fortfahren. Dies ist der letzte Versuch, die virtuellen Maschinen und die Hosts sauber herunterzufahren.

Sie können erneut die Zugangsdaten des vCenters mit dem Button „Check Values“ überprüfen.

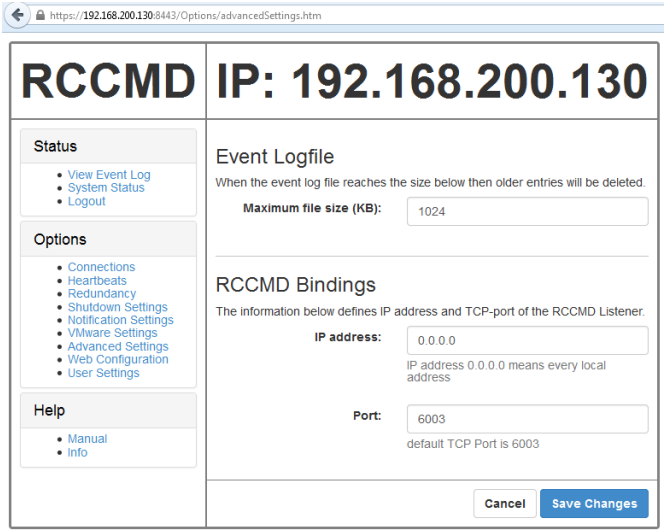

Abb. 193: RCCMD WebInterface – Advanced Settings

Im Menü „**Advanced Settings**“ können Sie die maximale Grösse des Event Logfiles definieren, bei der das Überschreiben älterer Einträge beginnt, die RCCMD Bindings für die IP-Adresse und den RCCMD Listener TCP Port.

Klicken Sie vor Verlassen des „Advanced Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Web Configuration**“ besteht die Möglichkeit, das HTTPS Protokoll zu deaktivieren, um nur mit dem HTTP Protokoll zu arbeiten. Ab der RCCMD Version 4.2.3.0 gibt es die Möglichkeit, die Standard Ports für HTTP bzw. HTTPS zu ändern und danach direkt den RCCMD WebIf neuzustarten.

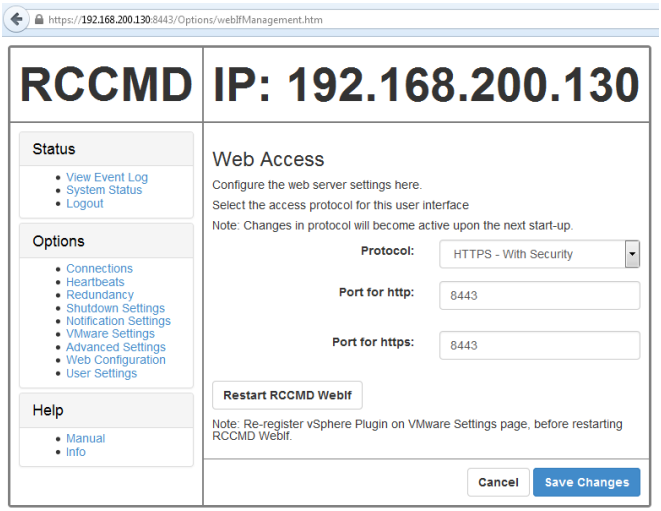

Abb. 194: RCCMD WebInterface – Web Access

Klicken Sie vor Verlassen des „Web Configuration“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern. Klicken Sie auf „Logout“, wenn Sie den Web Configurator nicht mehr benötigen.

Klicken Sie vor Verlassen des „Web Configuration“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**User Settings**“ können Sie das Standard Passwort für den Benutzer „admin“ wie gewünscht ändern und den RCCMD WebIf neustarten.

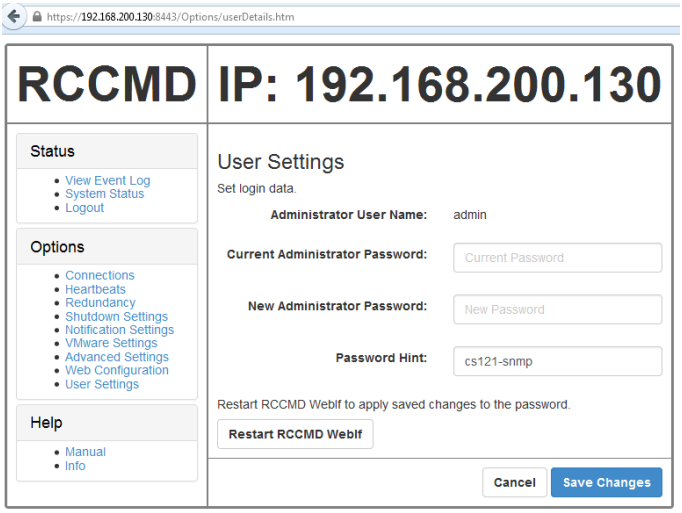

Abb. 195: RCCMD WebInterface – User Settings

Klicken Sie vor Verlassen des „User Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern. Klicken Sie auf „Logout“, wenn Sie den Web Configurator nicht mehr benötigen.

Im Menü „**Status, View Event Log**“ können Sie die Protokollierung der bisherigen Ereignisse einsehen.

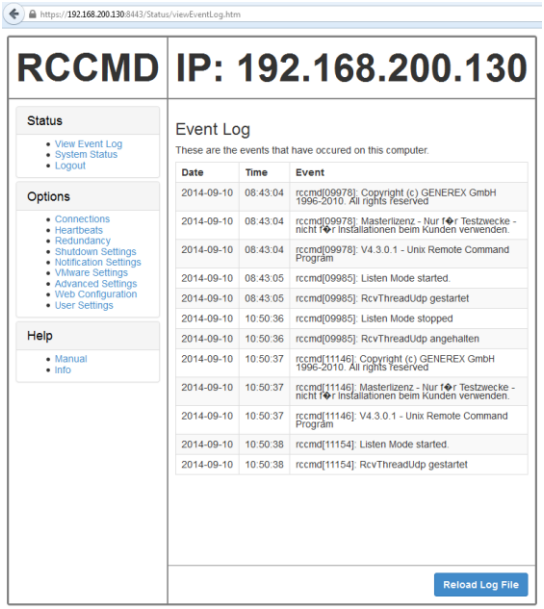
https://192.168.200.130:8443/Status/viewEventLog.htm
RCCMD
IP: 192.168.200.130
Status
View Event Log
System Status
Logout
Options
Connections
Heartbeats
Redundancy
Shutdown Settings
Notification Settings
VMware Settings
Advanced Settings
Web Configuration
User Settings
Help
Manual
Info
Event Log
These are the events that have occured on this computer.
Date
Time
Event
2014-09-10 08:43:04 rccmd[09978]: Copyright (c) GENEREX GmbH 1996-2010. All rights reserved
2014-09-10 08:43:04 rccmd[09978]: Masterlizenz - Nur f€r Testzwecke - nicht f€r Installationen beim Kunden verwenden.
2014-09-10 08:43:04 rccmd[09978]: V4.3.0.1 - Unix Remote Command Program
2014-09-10 08:43:05 rccmd[09985]: Listen Mode started.
2014-09-10 08:43:05 rccmd[09985]: RcvThreadUdp gestartet
2014-09-10 10:50:36 rccmd[09985]: Listen Mode stopped
2014-09-10 10:50:36 rccmd[09985]: RcvThreadUdp angehalten
2014-09-10 10:50:37 rccmd[11146]: Copyright (c) GENEREX GmbH 1996-2010. All rights reserved
2014-09-10 10:50:37 rccmd[11146]: Masterlizenz - Nur f€r Testzwecke - nicht f€r Installationen beim Kunden verwenden.
2014-09-10 10:50:37 rccmd[11146]: V4.3.0.1 - Unix Remote Command Program
2014-09-10 10:50:38 rccmd[11154]: Listen Mode started.
2014-09-10 10:50:38 rccmd[11154]: RcvThreadUdp gestartet
Reload Log File

Abb. 196: RCCMD WebInterface – Event Log

Im Menü „**Status, System Status**“ können Sie den aktuellen Status von RCCMD überprüfen, den Status updaten und den RCCMD Dienst neustarten bzw. stoppen und starten.

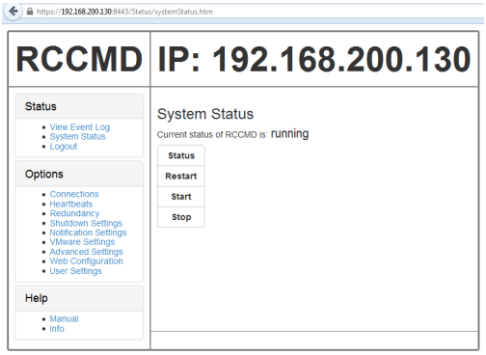

Abb. 197: RCCMD WebInterface – System Status

Im Menü „**Help**“ können Sie das RCCMD Benutzerhandbuch zu Ihrer Unterstützung aufrufen, können dem Link auf www.generex.de folgen und die Installer Version via „Info“ anzeigen.

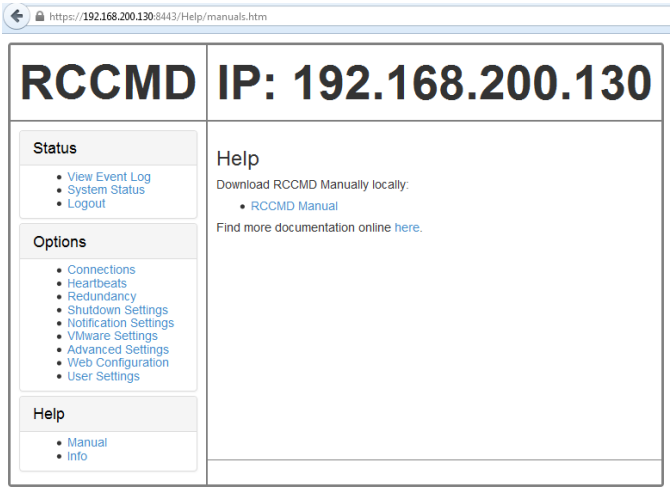

Abb. 198: RCCMD WebInterface – Help

Achtung: Bitte beachten Sie, dass die vMA nach einem Shutdown manuell gestartet werden muss!

4.2.7 Alternative RCCMD Konfiguration über Editor

Manuelles Bearbeiten der Konfigurationsdatei „rccmd.cfg“ (default /usr/rccmd).

```
########################################
# RCCMD Configuration (v3-default)
########################################

#
# Bind on Interface
# Defines on which interface we listen for incoming commands
# Default: 0.0.0.0 (All possible interfaces on this host)
ListenAddress=0.0.0.0
#
# Listen on Port
# Defines on which interface port we listen for incoming commands.
# Default: 6003
ListenPort=6003
#
# Enable UDP
# Defines if we should listen for rccmd (UDP) broadcasts
# Default: true
ListenUDP=true
#
# Access Control List
```

```
# A list of valid sender addresses, only its members can connect to us.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (Everyone is allowed to connect to us)
AllowedAddresses=
########################################
# Alive Check
#
# Enable Alive Check
# Defines if we should perform UPSMan alive checking.
# Default: false
AliveEnabled=false
#
# Alive Check Rate
# Defines the interval of UPSMan alive checking, in seconds.
# Default: 1800
AliveInterval=1800
#
# Alive Retry Rate
# Defines the number of UPSMan alive checking retries, in case of problems.
# Default: 0
AliveRetries=5
#
# Alive Check Group Members List
# A list of UPS device addresses that should be checked periodically.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (No alive checking)
AliveAddresses=
#
# Alive Program
# Full path to script that is executed when an alive check fails.
# Default: rccmd_notalive.sh
AliveProg=/usr/rccmd/rccmd_notalive.sh
########################################
# Redundancy Mode
#
# Enable Redundancy
# Defines if we should operate in redundancy mode.
# Requires an enabled <Alive Check> configuration.
# Default: false
RedundancyEnabled=false
#
# Redundancy Group Members List
# A list of redundancy group member addresses, must be also in <AliveAddresses>.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (No redundancy available)
RedundancyAddresses=
#
# Redundancy Level
# Defines how many of the <RedundancyAddresses> are redundant.
# Shutdown is executed when the number of shutdown requests exceeds this number.
# Default: 0 (No redundancy available)
RedundancyLevel=0
# Enable Redundancy Script
# Defines if we should NOT execute a script when redundancy suppresses a shutdown.
# Default: false.
RedundancyBatchSuppress=false
# Redundancy Script
```

```
# Full path to script that is executed when redundancy suppresses a shutdown.
# Default: ShutdownSuppressed.sh
RedundancyBatchFile=/usr/rccmd/ShutdownSuppressed.sh
# SSL encryption
# enables SSL encrypted messages RCCMD
SSL=false
# Rejection/Acceptance of expired Certificates
# disables SSL communication that try to use expired certificates
SSLRejectExpiredCert=false
ExecProg=/usr/rccmd/rccmd_execute.sh
########################################
vCenter=true
shutdownHosts=192.168.200.34|91
hostshutdownactive=true
ups_vm_name=vMA5.1
Key=secret
Language=english
vMotion=true
vCenterAddress=192.168.200.65
vMotionTimeout=92
```

5. RCCMD auf Citrix XEN Server

Die RCCMD Software auf XEN Server ist ein auf Linux basierter TCP Client, der das Empfangen von Shutdown Signalen von der UPSMAN Software, CS121 SNMP Adapter oder jeder anderen lizensierten RCCMD Anwendung.

RCCMD auf XEN Server läuft auf GNU Linux 2.6.18 oder höher, das die Basis der 2008 XEN Serverplattform ist.

Für die Installationsanleitung von RCCMD, schauen Sie bitte in das Kapitel 5.3 auf Seite 64. Im Folgenden beschreiben wir nur die speziellen Aspekte, die nur für XEN Server relevant sind.

Installation:

Da der XEN Server keine grafische Oberfläche unterstützt, der Download der RCCMD Software für XEN Server von der GENEREX Webseite oder anderen Seiten, ist es nicht einfach, es sei denn, Sie haben einige Extra Tools installiert, z. B. den Befehlszeilen-Browser *Wget*.

Eine zusätzliche Schwierigkeit ist, dass auf XEN Server kein FTP Server aktiv ist, sodass ein Transfer eines RCCMD Download-Paketes auch nicht möglich ist. Darum empfehlen wir, eine lokale Schnittstelle, z.B. ein CD-ROM Laufwerk, auf Ihrem XEN Server zu nutzen oder mit einem USB Stick zu arbeiten.

- Laden Sie RCCMD mit ihrer Lizenznummer (nicht älter als 2 Jahre) von der GENEREX Webseite herunter, und extrahieren Sie das TAR File. Kopieren Sie die Files auf eine CD-R, und legen Sie die CD in das Laufwerk auf Ihrem XEN Server. Alternativ können Sie die UPSMAN CD-ROM Version 5.48 oder höher nutzen.

- Loggen Sie sich als Root ein, und mounten Sie die CD-ROM auf Ihrem XEN Server: Geben Sie `mount/dev/cdrom/media` ein. Sie werden folgende Antwort vom System erhalten: `mount: block device /dev/cdrom is write protected, mounting read-only`
- Wechseln Sie zu dem CD-ROM Verzeichnis mit: `cd/media` – mit `ls` können Sie sich die Files der CD-ROM anzeigen lassen. Wechseln Sie in das Verzeichnis UNIX (UPSMAN CD-ROM) oder GENEREX. Darin befindet sich das Installations-File "install".
- Starten Sie die Installation mit der Eingabe: `./install` und folgen Sie den Anweisungen auf dem Bildschirm, die identisch zur Installation von RCCMD auf UNIX ist.
- Nach dem die Installation beendet ist, wird ein neuer Prozess auf Ihrem XEN Server laufen: `:/rccmd -l` , was bedeutet, dass das System nun bereit ist.
- **Achtung**: Der XEN Server hat standardmässig eine aktive Firewall, die keine "remote" RCCMD Signale zulässt. Um die Firewall zu öffnen, müssen die *iptables* (`/etc/sysconfig#`) editiert werden.

Firewall Konfiguration:

Fügen Sie die folgenden *Lines* in `/etc/sysconfig/iptables` **vor** der letzten *REJECT* Regel hinzu:

```
-A RH-Firewall-1-INPUT -p udp --dport 6003 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp --dport 6003 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/sysconfig/iptables" [readonly] 25L, 1215C
```

Abb. 199: Firewall Konfiguration

Starten Sie die *iptables* wie folgt neu:

```
/etc/init.d/iptables restart
```

RCCMD ist nun im Lauscher-Modus konfiguriert, und wird das File *shutdown.sh* auf Ihrem XEN Server starten, wenn ein CS121 Adapter oder UPSMAN ein RCCMD Shutdown Signal sendet. Das File *shutdown.sh* führt ein *init0 shutdown* auf Ihrem XEN Server aus. Ändern Sie das File, wenn Sie eine andere Shutdown Prozedur verwenden möchten.

Hinweis:

Es wird empfohlen, RCCMD auch auf den virtuellen Gast-systemen zu installieren und diese VOR dem physikalischen Hostrechner herunterzufahren. Dies garantiert ein sauberes Herunterfahren der virtuellen Maschinen und verhindert den möglichen Datenverlust durch ein nicht erfolgreiches Hibernating.

6. RCCMD auf MAC OS 10.X

Hinweis:

Der RCCMD Installer verwendet die von uns mitgelieferte Java Runtime Version, die nur für die Installation bzw. Deinstallation verwendet wird. Zusätzlich verwendet der RCCMD Web Configurator einen Java Webserver (jetty). Wenn Sie RCCMD ohne Java verwenden möchten, entfernen Sie den Eintrag /System/Library/StartupItems/RccmdWebIf (bis MAC OS 10.5) oder (ab MAC OS 10.5) /Library/LaunchDaemons/de.generex.rccmdWebif.plist

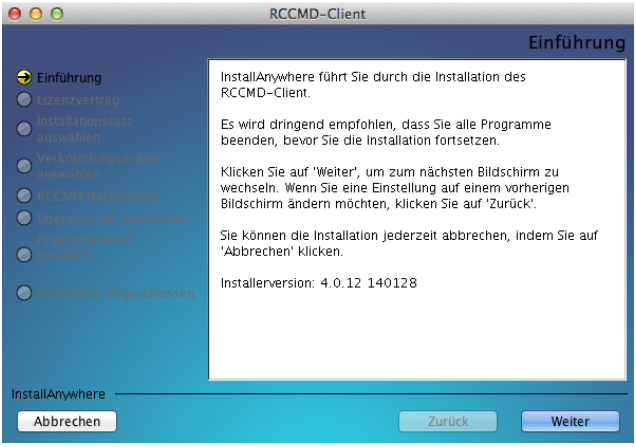
RCCMD-Client
Einführung
Einführung
Lizenzvertrag
Installationssatz auswählen
Verknüpfungsordner auswählen
RCCMD Nachrichten
Übersicht vor Installation
Programm wird installiert
Installation abgeschlossen
InstallAnywhere führt Sie durch die Installation des RCCMD-Client.
Es wird dringend empfohlen, dass Sie alle Programme beenden, bevor Sie die Installation fortsetzen.
Klicken Sie auf 'Weiter', um zum nächsten Bildschirm zu wechseln. Wenn Sie eine Einstellung auf einem vorherigen Bildschirm ändern möchten, klicken Sie auf 'Zurück'.
Sie können die Installation jederzeit abbrechen, indem Sie auf 'Abbrechen' klicken.
Installerversion: 4.0.12 140128
InstallAnywhere
Abbrechen
Zurück
Weiter

Abb. 200: RCCMD Installation-Einführung

Sie benötigen einen speziellen Lizenz-Schlüssel für die RCCMD Software, den Sie an dem “RX3” im ersten Teil des Schlüssels erkennen können. In den meisten Fällen muss die Lizenz separat bestellt werden.

Abb. 201: RCCMD Lizenz Schlüssel Eingabe

Wählen Sie die Features, die Sie installieren möchten.

Abb. 202: RCCMD Installationssatz Auswahl

Wählen Sie einen Aliasordner.

Abb. 203: RCCMD Aliasordner Auswahl

Wählen Sie die gewünschten Wiedergabemöglichkeiten.

Abb. 204: RCCMD Nachrichten

Abb. 205: Prä-Installations-Übersicht

Klicken Sie auf „Installieren“, um die Installation abzuschliessen.

Akzeptieren Sie folgende Defaultwerte für das Web-Interface, oder wählen Sie eigene.

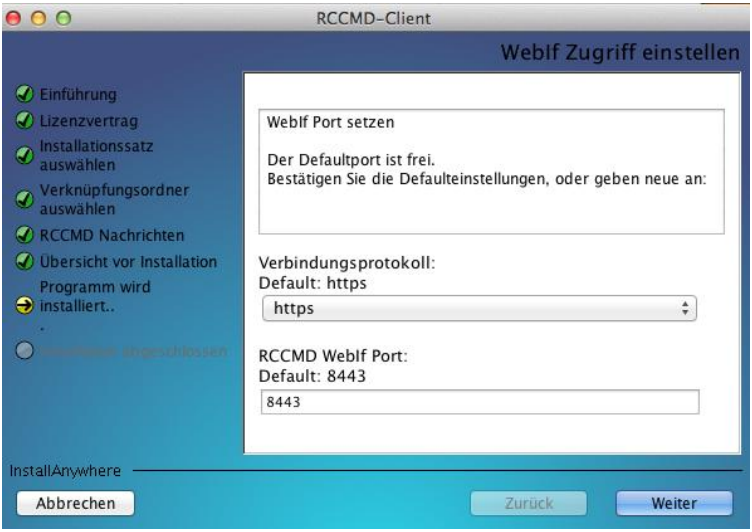

Abb. 206: WebIf Zugriff einstellen

Setzen Sie ein Passwort für das RCCMD Webinterface.

Abb. 207: Kennworteingabe

Geben Sie ein Passworthinweis ein.

Abb. 208: Passworthinweis-Eingabe

Beachten Sie den folgenden Hinweis.

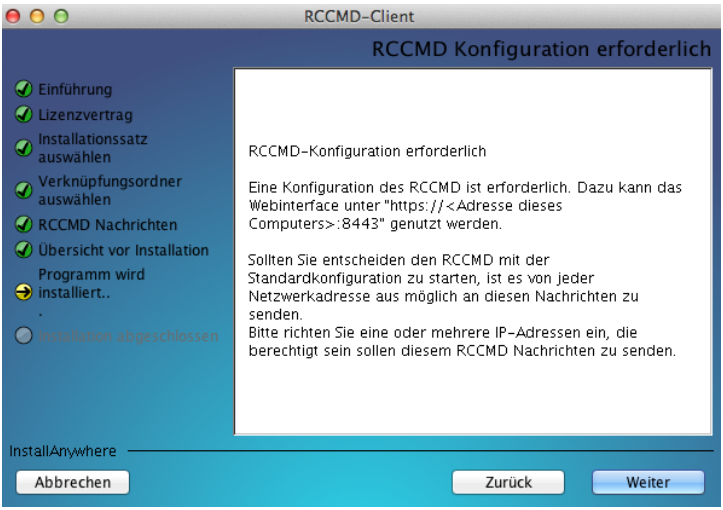
RCCMD-Client
RCCMD Konfiguration erforderlich
Einführung
Lizenzvertrag
Installationssatz auswählen
Verknüpfungsordner auswählen
RCCMD Nachrichten
Übersicht vor Installation
Programm wird installiert..
Installation abgeschlossen
RCCMD-Konfiguration erforderlich
Eine Konfiguration des RCCMD ist erforderlich. Dazu kann das Webinterface unter "https://<Adresse dieses Computers>:8443" genutzt werden.
Sollten Sie entscheiden den RCCMD mit der Standardkonfiguration zu starten, ist es von jeder Netzwerkadresse aus möglich an diesen Nachrichten zu senden.
Bitte richten Sie eine oder mehrere IP-Adressen ein, die berechtigt sein sollen diesem RCCMD Nachrichten zu senden.
InstallAnywhere
Abbrechen
Zurück
Weiter

Abb. 209: RCCMD Konfiguration erforderlich

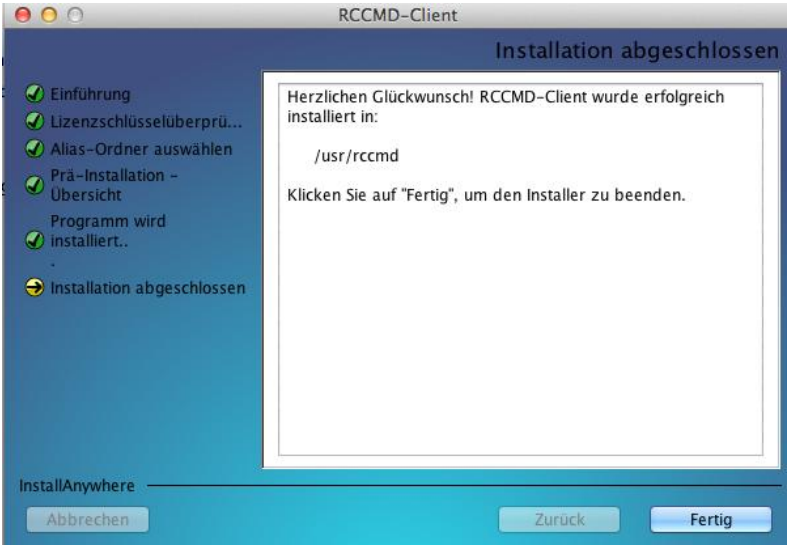

Abb. 210: Installationssabschluss

6.1 RCCMD WebInterface (ab Version 4.2.0.0)

Ab der RCCMD Version 4.2.0.0 verfügt RCCMD über ein eigenes Webinterface, das die webbasierte Konfiguration bzw. Steuerung aus der Ferne ermöglicht. Nach der erfolgreichen Installation, öffnet sich automatisch der Standardwebbrowser Ihres Betriebssystems.

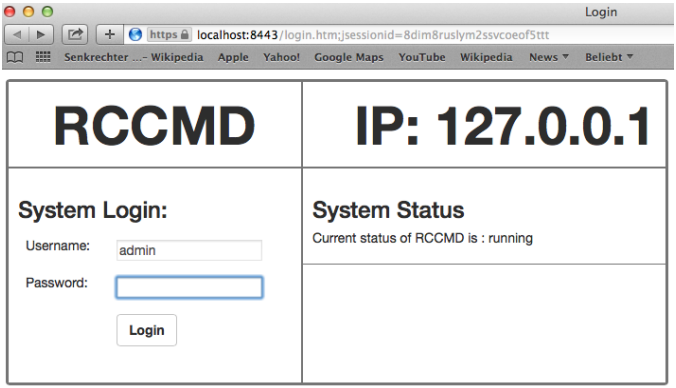

Abb. 211: RCCMD WebInterface

Im Menü „**Connections**“ können Sie die IP-Adressen der berechtigten RCCMD Sender (CS121/UPSMAN) eintragen. Klicken Sie auf „Insert“, um die IP-Adresse des ersten Senders einzutragen. Klicken Sie auf „Remove“, wenn Sie die eingetragene IP-Adresse herausnehmen möchten. Klicken Sie auf „Edit“, wenn Sie die eingetragene IP-Adresse bearbeiten möchten.

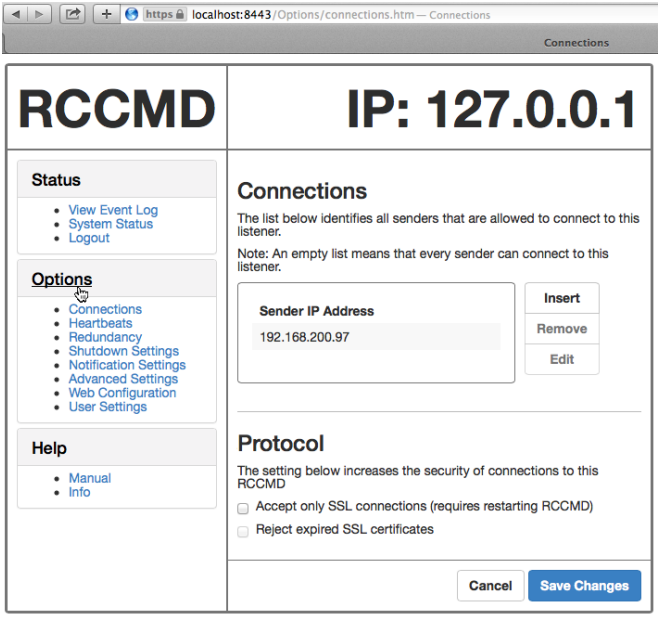

Abb. 212: RCCMD WebInterface – Connections

Achtung: **Wenn Sie hier keine Adresse eintragen, ist jeder Server in der Lage, einen Shutdown an diesen Client zu senden.**

Unter „**Protocols**“ kann definiert werden, ob RCCMD mit SSL Zertifikaten verwendet wird. Aktivieren Sie „Reject expired SSL certificates“, wenn Sie Verbindungen mit abgelaufenen SSL Zertifikaten ablehnen wollen. Weitere Informationen für RCCMD mit SSL finden Sie in Kapitel 6.6.1.

Klicken Sie vor Verlassen des „Connections“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Heartbeats**“ kann die Funktion „UPSMAN Alive Check“ aktiviert werden.

Dieser Check ist ein Signal, das an den CS121 oder UPSMAN via Port 5769 gesendet wird, um zu prüfen, ob der UPSMAN noch USV Daten hat. Wenn nicht, wird das Script File “Alive.Bat” ausgeführt, das eine entsprechende Nachricht als Pop-Up bringt.

Die Funktion “by the use CS121/UPSMAN Traps” ermöglicht UPSMAN/RCCMD/UNMS Meldungen, die den USV Status als Nachricht anzeigen. Wenn aktiviert, wird diese Funktion eine lokale Nachricht bringen, wenn der USV Status des UPSMAN/RCCMD Servers sich verändert.

Die Funktion „by polling CS121/UPSMAN every x seconds“ ermöglicht die reine Signalabfrage, ohne das Empfangen von USV-Werten bzw. Nachrichten.

Die Polling Rate (Standard 1800 Sekunden) definiert den Interval der UPSMAN Abfrage, connection retries (Verbindungswiederholungen, Standard 100) bedeutet, das nach 100 erfolglosen Verbindungsversuchen ein Alarm ausgelöst wird.

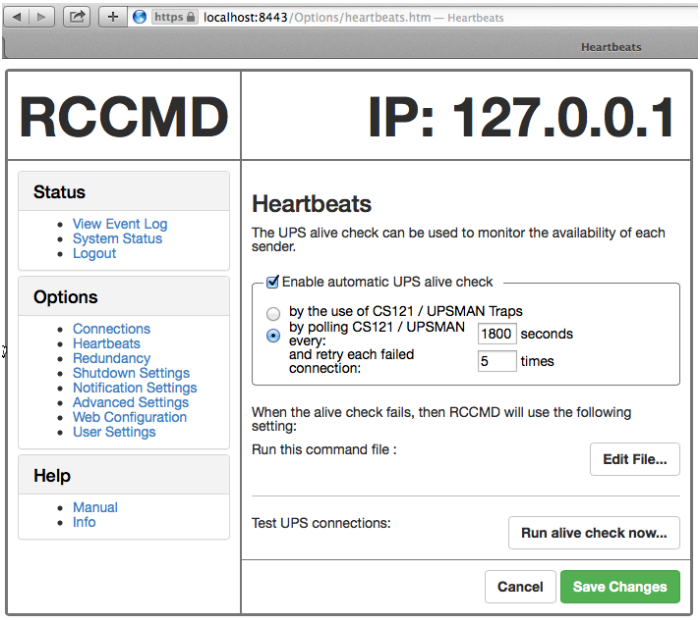

Abb. 213: RCCMD WebInterface – Heartbeats

Wenn Sie auf “Run alive check now…” klicken, wird das UPSMAN Alive Checking von der eingetragenen IP-Adresse gestartet (der Port 5769 wird getestet).

Klicken Sie vor Verlassen des „Heartbeats“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Redundancy**“ kann die Redundanz Management Funktion aktiviert werden. Der Redundanz Level definiert die Anzahl der redundanten Sender in der Redundanz Gruppe. Das bedeutet, dass bei einem Redunz Level von 1 beide RCCCMD Sender (CS121/UPSMAN) einen Shutdown gesendet haben müssen, bevor RCCMD seine Shutdown Sequenz startet.

Wenn RCCMD einen Shutdown unterdrückt, erhalten Sie eine Nachrichten Box aus der „Suppressed.bat“, die Sie verändern können, wenn Sie auf „Edit File...“ klicken.

Bitte beachten Sie, dass für das Zurücksetzen des Redundanz Alarms eine Event Konfiguration auf dem Sender (CS121/UPSMAN) erforderlich ist. Die Funktion „Send RCCMD cancle shutdown“ kann verwendet werden, um automatisch einen vorher abgesendeten Shutdown zu verwerfen. Wenn ein Shutdown unterdrückt wurde, wegen der zu diesem Zeitpunkt noch vorhandenen Redundanz, das Problem aber zwischenzeitlich an der USV gelöst wurde, kann mittels einem „Send RCCMD cancel shutdown“ der Alarm zurückgesetzt werden. Durch diesen Befehl wird der RCCMD Client, der vorher das Shutdownsignal erhalten hat, aufgefordert, dieses wieder rückgängig zu machen.

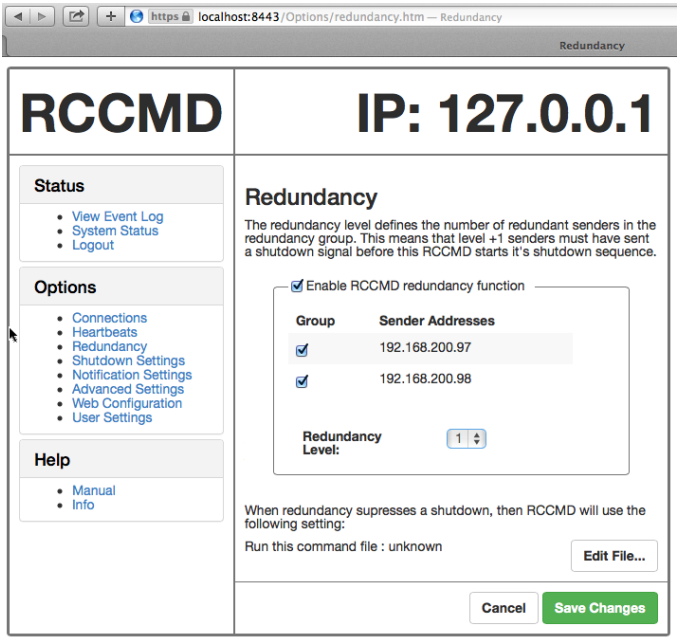

Abb. 214: RCCMD WebInterface – Redundancy

Klicken Sie vor Verlassen des „Redundancy“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Shutdown Settings**“ können Sie die Shutdown Sequenz verändern bzw. erweitern. Als Standard wird die rccmd_shutdown.sh verwendet:

#!/bin/sh

This script is created by RCCMD shutdown sequence configuration.

This script is called by rccmd after receiving

the "SHUTDOWN" command from the network.

available command are:

shutdown -h now &

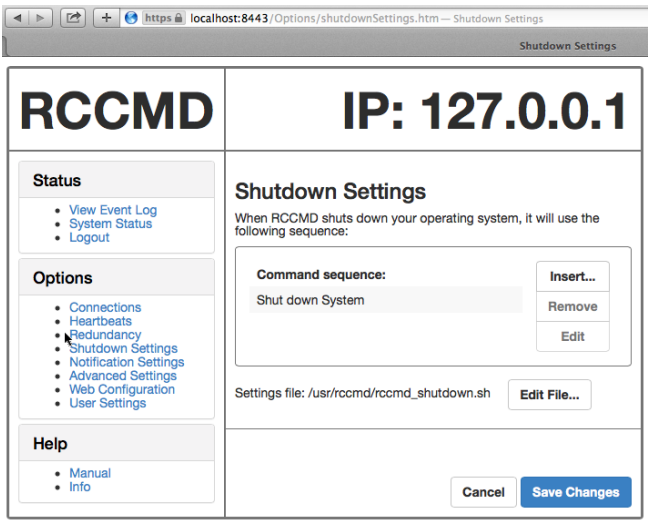

Abb. 215: RCCMD WebInterface – Shutdown Settings

Im Menü „**Notification Settings**“ können Sie die entsprechenden Standard Bat-Files für E-Mail, Message (Nachrichten) und Execute (auszuführende Kommandos) verändern bzw. erweitern, wenn Sie auf „Edit File...“ klicken.

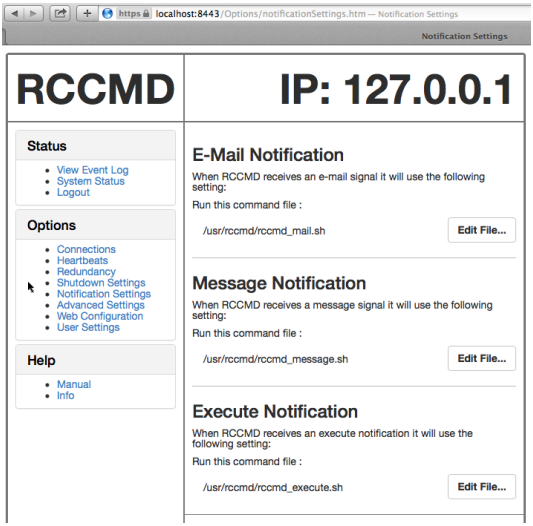

Abb. 216: RCCMD WebInterface – Notification Settings

Klicken Sie vor Verlassen des „Notification Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Advanced Settings**“ können Sie die maximale Grösse des Event Logfiles definieren, bei der das Überschreiben älterer Einträge beginnt, die RCCMD Bindings für die IP-Adresse und den RCCMD Listener TCP Port.

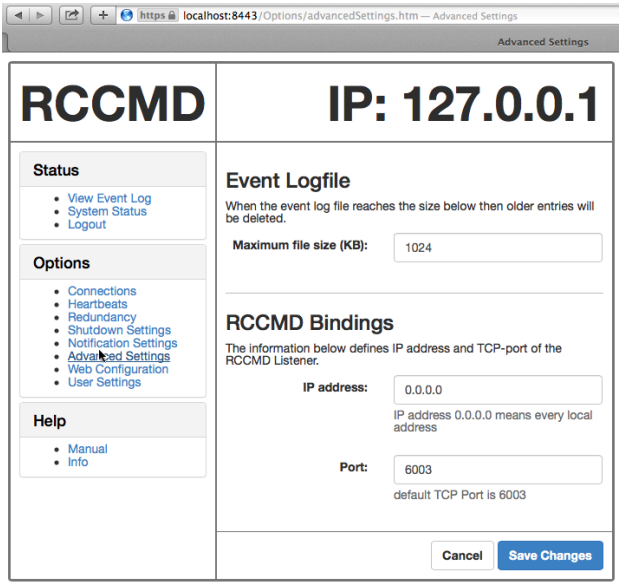

Abb. 217: RCCMD WebInterface – Advanced Settings

Klicken Sie vor Verlassen des „Advanced Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**Web Configuration**“ besteht die Möglichkeit, das HTTPS Protokoll zu deaktivieren, um nur mit dem HTTP Protokoll zu arbeiten. Ab der RCCMD Version 4.2.3.0 gibt es die Möglichkeit, die Standard Ports für HTTP bzw. HTTPS zu ändern und den RCCMD WebIf neuzustarten.

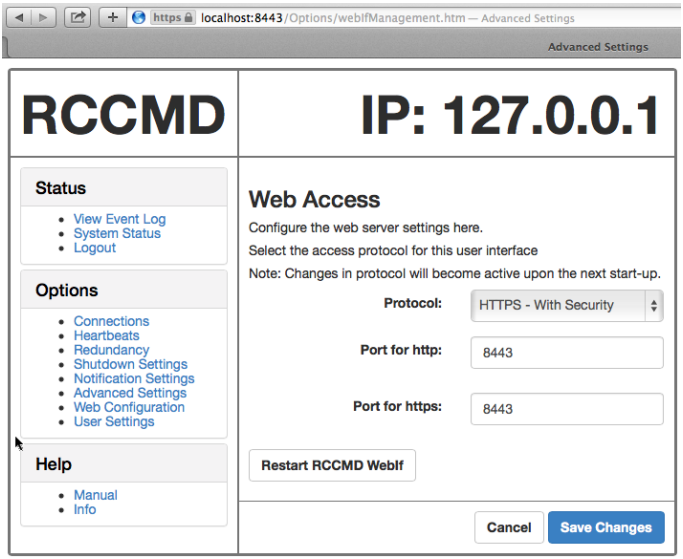

Abb. 218: RCCMD WebInterface – Web Access

Klicken Sie vor Verlassen des „Web Configuration“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Im Menü „**User Settings**“ können Sie das Standard Passwort für den Benutzer „admin“ wie gewünscht ändern und den RCCMD WebIf neuzustarten.

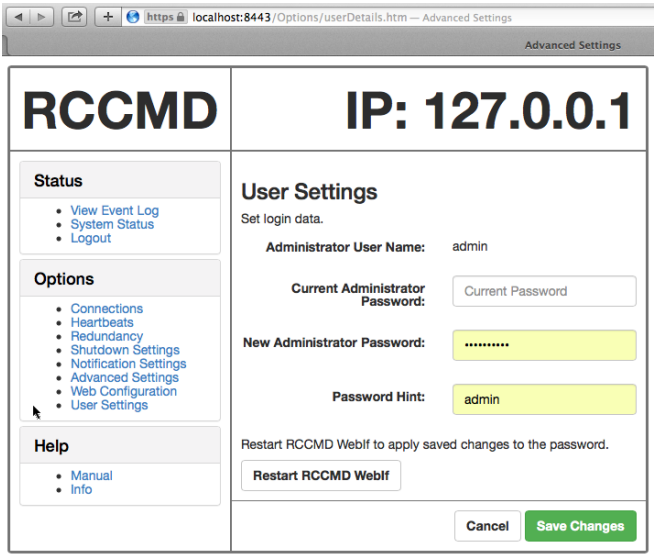

Abb. 219: RCCMD WebInterface – User Settings

Klicken Sie vor Verlassen des „User Settings“ Menüs auf „Save Changes“, um Ihre Änderungen zu sichern.

Klicken Sie auf „Logout“, wenn Sie den RCCMD Web Configurator nicht mehr benötigen.

Im Menü „**Status, View Event Log**“ können Sie die Protokollierung der bisherigen Ereignisse einsehen.

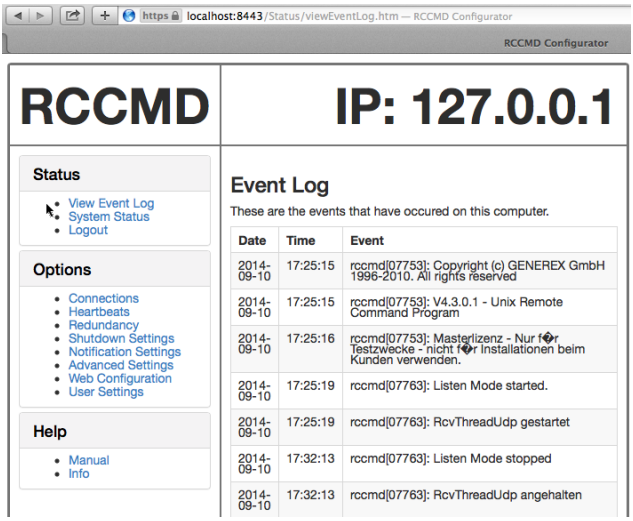

Abb. 220: RCCMD WebInterface – Event Log

Im Menü „**Status, System Status**“ können Sie den aktuellen Status von RCCMD überprüfen, den Status updaten und den RCCMD Dienst neustarten bzw. stoppen und starten.

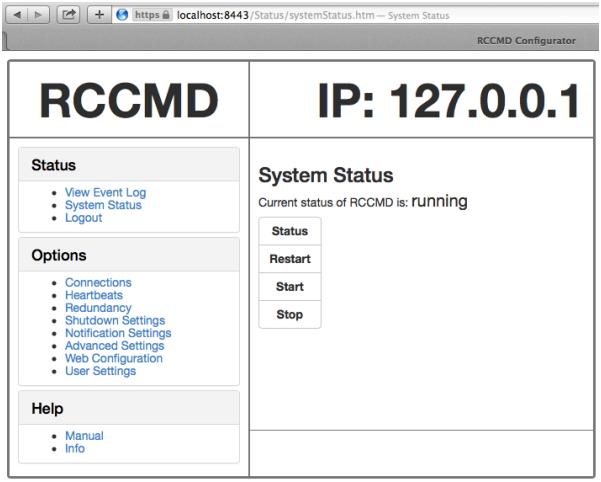

Abb. 222: RCCMD WebInterface – System Status

Im Menü „**Help**“ können Sie das RCCMD Benutzerhandbuch zu Ihrer Unterstützung aufrufen, können dem Link auf www.generex.de folgen und die Installer Version aufrufen.

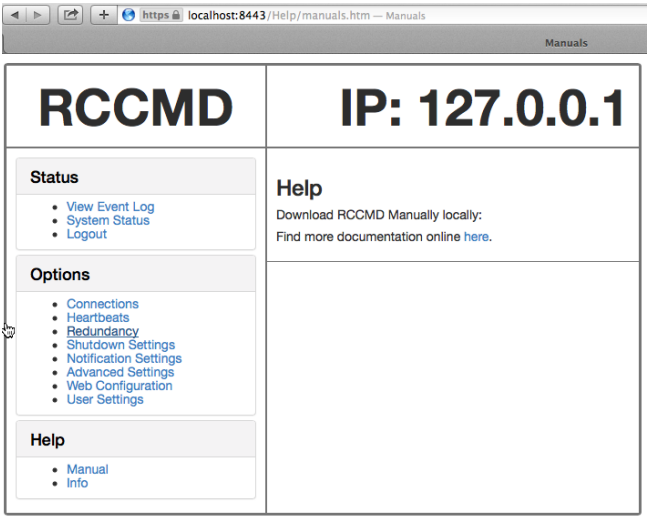

Abb. 223: RCCMD WebInterface – Help

6.2 RCCMD WebInterface Remote Zugriff

Ab der RCCMD Version 4.2.0.0 verfügt RCCMD über ein eigenes Webinterface, dass den Remote Zugriff ermöglicht. Bitte beachten Sie, dass der Firewall Port 8443 TCP freigeschaltet sein muss. Geben Sie in einem Webbrowser Folgendes ein, um sich remote auf den Rechner zu verbinden, auf dem RCCMD installiert wurde

https://IP-Adresse des RCCMD Rechners:8443

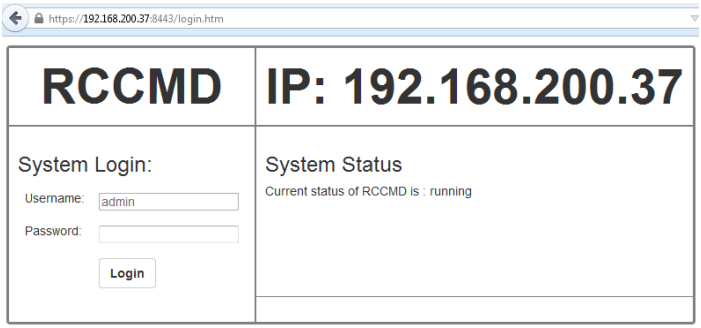

Abb. 224: RCCMD WebInterface – Remote Zugriff

Nun besteht die Möglichkeit, die Konfiguration bzw. Steuerung aus der Ferne auszuführen.

Fügen Sie die IP-Adresse des RCCMD Servers hinzu, der authorisiert ist, ein Shutdown Signal zu diesem Client zu senden.

6.3 Alte RCCMD Konfiguration auf MAC OSX

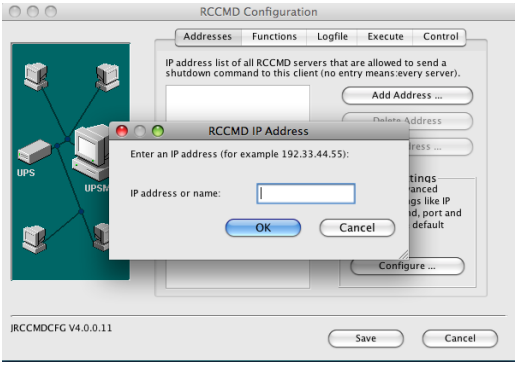

Abb. 226: RCCMD IP Adressen Fenster

Achtung: **Wenn Sie keine Adresse eintragen, ist automatisch jeder Server authorisiert, ein Shutdown Signal zu senden. Wenn mehr als ein CS121 oder UPSMAN im Netzwerk existieren, also**

eine Redundanz Situation, müssen Sie mehrere Adressen als authorisierte Sender eintragen.

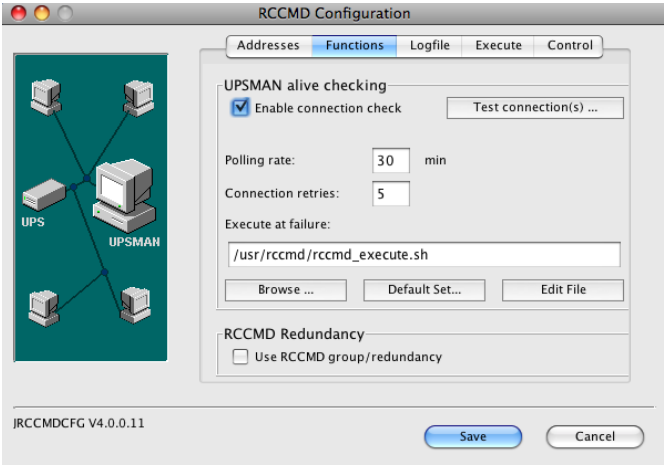

Abb. 227: RCCMD Konfigurations-Fenster „Functions“

Wenn Sie die Funktion “UPSMAN Alive Checking” nutzen möchten (empfohlen), haken Sie die entsprechende Box an. Dieser Check ist ein Signal, dass an den CS121 oder UPSMAN via Port 5769 gesendet wird, um zu prüfen, ob der UPSMAN noch USV Daten hat. Wenn nicht, wird das Script File “rccmd_notalive.sh” ausgeführt, das eine entsprechende Nachricht als Pop-Up bringt. Die *Polling Rate* (Standard 30 Minuten) definiert den Interval der UPSMAN Abfrage, *connect retries* (Verbindungswiederholungen, Standard 5) bedeutet, das nach 5 erfolglosen Verbindungsversuchen ein Alarm ausgelöst wird.

Die Funktion “Use RCCMD Traps” ermöglicht UPSMAN/RCCMD/UNMS Meldungen, die den USV Status als Nachricht anzeigt. Wenn aktiviert, wird diese Funktion eine lokale Nachricht bringen, wenn der USV Status des UPSMAN/RCCMD Servers sich verändert.

Wenn Sie auf “Test connections…” klicken, wird das UPSMAN Alive Checking von der eingetragenen IP-Adresse gestartet (der Port 5769 wird getestet).

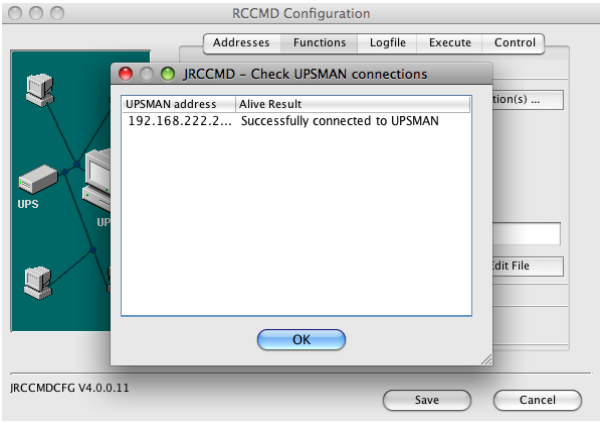

Abb. 228: RCCMD Check UPSMAN Verbindungen

Wenn Sie auf “Browse…” klicken, werden Sie eine Auswahl der Standard SH-Files erhalten.

Wenn Sie auf „Default Setting“ klicken, werden Sie zurück zum „rccmd_notalive.sh“ File gelangen.

Bei einem Fehler von dem UPSMAN Alive Check können Sie eine auszuführende Datei konfigurieren oder das Standard File editieren.

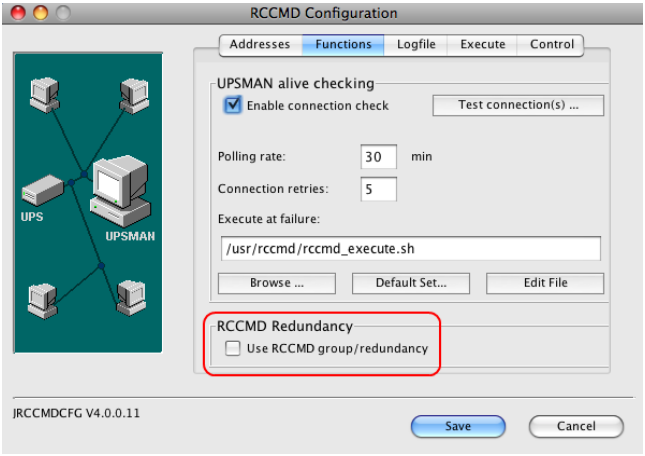

Abb. 229: RCCMD Redundanz

Bei der USV Installation bietet RCCMD eine Redundanz Management Funktion wie folgt an:

Jede USV muss mit einem CS121 oder einem UPSMAN Software Computer ausgestattet sein. Wenn Sie die Box “Use RCCMD group/redundancy” anhaken, gelangen Sie zu einem Menü, welcher CS121/UPSMAN diesen RCCMD Client versorgt. Z.B.: Wenn 4

CS121/UPSMAN in 4 USVen installiert sind, dann kann jeder ein Shutdown Signal zu diesem RCCMD Client absetzen.

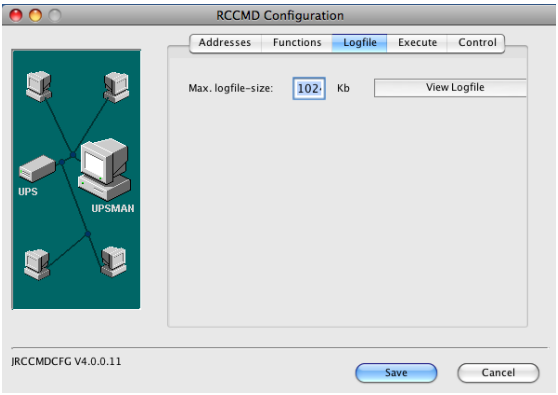

Abb. 230: RCCMD Konfigurations-Fenster „Logfile“

Sie können die Log File Grösse konfigurieren und die auszuführenden Files editieren.

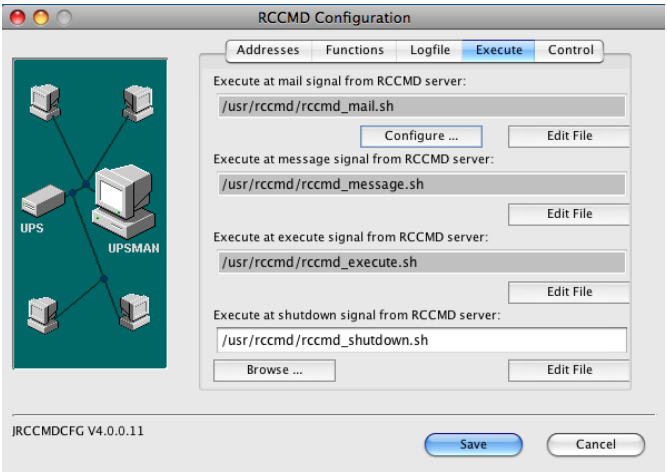

Abb. 231: RCCMD Konfigurations-Fenster „Execute“

Wenn Sie auf “Configure…” klicken, können Sie die Email Einstellungen vornehmen und die Mailfunktion von RCCMD nutzen.

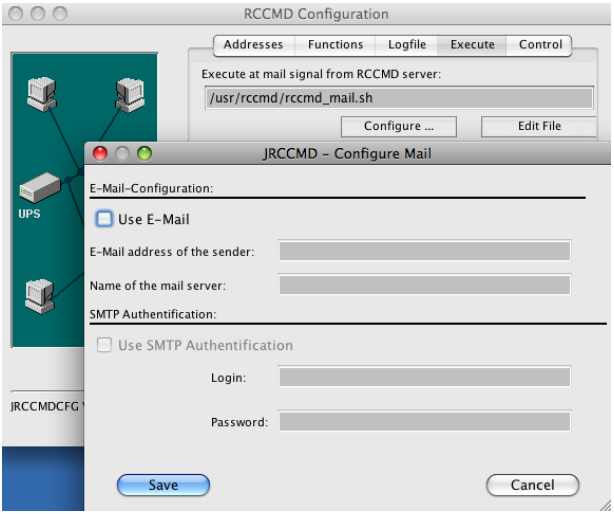

Abb. 232: RCCMD E-Mail-Konfiguration

Ab der RCCMD Version 4.0.2.0 gibt es auch eine grafische Konfiguration der Shutdown Sequenz.

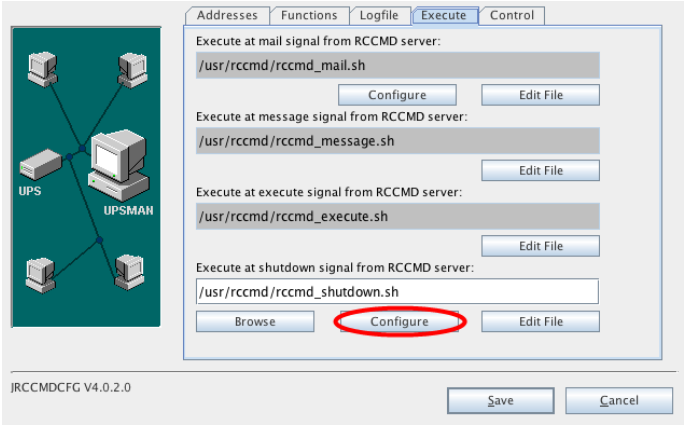

Abb. 233: Konfiguration – RCCMD Shutdown.sh

Klicken Sie auf „Configure“, um die Shutdown Sequenz zu öffnen.

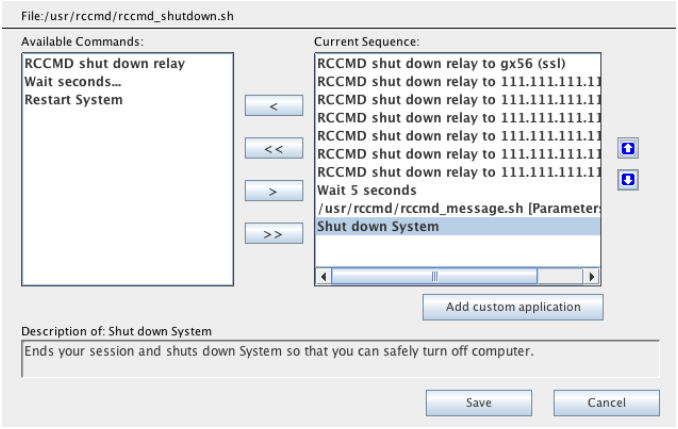

Abb. 234: Konfiguration – RCCMD Shutdown Sequenz

Die folgenden Befehle sind für die Shutdown Sequenz Konfiguration erhältlich:

RCCMD shutdown relay: Leitet einen RCCMD Shutdown Befehl an eine andere Workstation weiter (siehe auch Kapitel 5.4, Seite 75).

Wait seconds...: Warten eines Zeitraums in Sekunden, bis das nächste Kommando ausgeführt wird.

Restart System: Beendet Ihre Sitzung, fährt das System herunter und startet es neu.

Shutdown System: Beendet Ihre Sitzung und fährt das System herunter, sodass Sie sicher die Stromzufuhr unterbrechen können.

Über den „Control“ Button gelangen Sie zu der folgenden Maske:

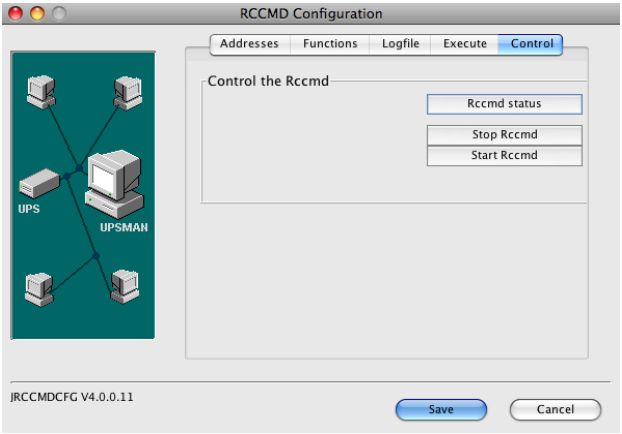

Abb. 235: RCCMD Control

7. RCCMD auf NovellNetWare

Downloaden Sie das RCCMD Paket netwar5.zip. Extrahieren Sie es in einen beliebigen Ordner auf Ihrem Windows oder Novell Server. Erstellen Sie ein Verzeichnis „UPS“ auf dem Netware SYS Volume (z. B. F:\UPS). Kopieren Sie die extrahierten Files in dieses Verzeichnis. Führen Sie das Folgende aus:

```
load rccmd.nlm -l -a load down.ncf
```

Wenn Sie den Hilfs-Parameter “?” auf einer NovellNetWare Konsole eingeben, erhalten Sie folgende Hinweise:

```
Possible parameters:

 -l
     listen. waits for a command from RCCMD sender

 -s
     sends a ping to a listening program

 -se <command> <param>
     sends a command to a listening program

 -p  <port>
     Portadress (Defaultadress = 6003)

 -a  <ipaddress>
     Address in IP Format. Ex. -a 192.10.20.30 (max.
10)

 -t  <timeout>
     Time in Seconds (Defaulttimeout = MAX_TIMEOUT)

 -?
     this help

Supported Commands (for use with -se argument):

 SHUTDOWN
          This will call the configured shutdown-
batchfile (default: shutdown.bat)

 EXECUTE
          This will call the execute.bat file

 MSG_TEXT
```

```
          This will call the message.bat file
<text, unrestricted word count>

 MSG_ID <ID>
          This will call the message.bat file
<message parameters, seperated by blanks>

 LOG_TEXT
          This will write to configured log-file
(default: rccmd.log) <text, unrestricted word count>

 LOG_ID <ID>
          This will write to configured log-file
(default: rccmd.log) <message parameters, seperated
by blanks>

Examples:

 load rccmd.nlm -s -a 192.10.200.52 -a 192.10.200.53
 load rccmd.nlm -s -a 192.10.200.52 -a 192.10.200.53
-t 10
 load rccmd.nlm -se "SHUTDOWN" -a 192.10.200.52

 load rccmd.nlm -se "EXECUTE" -a 192.10.200.52
 load rccmd.nlm -se "MSG_TEXT this is a message" -a
192.10.200.52
 load rccmd.nlm -l
 load rccmd.nlm -l -a 192.10.200.52 -a 192.10.200.53
 load rccmd.nlm -l -a 192.10.200.52

If you have added a search path i.e.: "search add
sys:rccmd",
otherwise you have to use the absolute path.

 load sys:rccmd\rccmd.nlm -l
```

Um RCCMD im Lauscher Modus zu starten, geben Sie bitte Folgendes ein:

load <path> RCCMD -l [-a 192.200.100.10] [-p 6003] load <path> shutcmd.nlm –f

Optionale Parameter:

-a <address> TCP/IP Adresse vom RCCMD Master, der das Signal sendet

-p <port> (optional) TCP-Port Adresse, auf den der Master das Signal sendet

Um RCCMD im Sender Modus zu starten, tragen Sie Folgendes in Ihren Shutdown-Job ein:

load RCCMD -s -a <address> [-p 6003]

Tragen Sie die IP-Adresse der Workstation ein, der Sie das Signal senden möchten (Workstations im Lauscher Modus mit einem aktiven RCCMD)

Optionale Parameter:

-p <port> TCP-Port, der das RCCMD Signal nutzt

Die Option "-a" kann mehrmals verwendet werden, wenn ein Shutdown auf Remote Netzwerk Servern ausgeführt werden soll.

Beispiel: (Pfad <path> = sys:\ups\upsman\rccmd.nlm)

load <path> RCCMD.NLM –s –a 192.168.210.3 -a 192.168.210.4 -a 192.168.210.10

...etc. bis unendlich

unload RCCMD

load <path> RCCMD.NLM –s –a 192.168.210.8...etc.

unload RCCMD

Bitte benutzen Sie den Lizenzschlüssel nicht mehr als einmal. Wenn Sie mehrere RCCMD Module für Shutdowns installieren möchten, benötigen Sie weitere Lizenzen, die Sie bei Ihrem USV Händler erhalten können.

rccmd.nlm

Modul für den Multiserver Shutdown in IP-Netzwerken. Das RCCMD.NLM beinhaltet verschiedene Befehlszeilen Parameter, die entweder im Sender Modus oder im Lauscher Modus verwendet werden:

rccmd -? Help

rccmd -s Sending off a "ping" signal to a waiting program

rccmd -l Waiting for a "ping" signal. A command can be executed after the reception of the "ping" signal.

rccmd –p Setting the port address (default = 6003).

rccmd –a Address in IP format e.g. 192.168.202.1

rccmd –t Time in seconds until a connection will be established. (default timeout = 10)

Example:

load sys:ups\rccmd.nlm -s -a 192.168.202.1 [-a 192.168.202.1]

load sys:ups\rccmd.nlm -s -a 192.168.202.1 -t 10

load sys:ups\rccmd.nlm -l -a 192.168.202.1 shutcmd.nlm [/para]

rccmdipx.nlm

Dies ist ein Modul speziell für IPX Netzwerke. Das Modul sendet einen Shutdown Befehl (oder jeden anderen Konsolen Befehl) direkt zu jeden IPX Server Namen. Bitte starten Sie RCCMDIPX auf allen Novell Konsolen. Das Modul muss auf beiden Servern geladen werden:

Benennen Sie die Datei um von RCCMDIPX zu RCCMS.NLM 2. Laden Sie RCCMD wie folgt:

rccmd <server name> <console command>

Als Servername muss ein gültiger Name aus der Netzwerk Umgebung angegeben werden, als Befehl ein gültiger NetWare-Befehl.

Beispiel:

1. load sys:ups\rccmdipx (or load RCCMD if RCCMDIPX.NLM is renamed to RCCMD.NLM)

2. rccmd gnw1 forcedown

or 1. load sys:ups\rccmdipx

2. rccmd gnw1 sys:ups\down.ncf

Anstelle des alten Down Befehls (clib.nlm Files), sollte der Forcedown Befehl benutzt werden.

Mehrfacher Start von RCCMD auf Novell

Der Multi-Start von RCCMD auf Novell ist relativ einfach zu handhaben. Mehrere RCCMD Clients sollten mit folgendem Befehl gestartet werden:

load rccmd.nlm -l -a load down.ncf

Die Syntax lautet wie folgt:

LOADING RCCMD.NLM -L(Lauscher) -A(IP-Adresse des UPSMAN/CS121/RCCMD Senders) COMMAND (Auszuführender Befehl)

Beispiel:

LOAD RCCMD.NLM -L -A 192.168.10.2 LOAD DOWN.NCF

In diesem Szenario soll das “down.ncf” File ausgeführt werden, das zu einem sofortigen Shutdown des Client Computers führt, wenn das RCCMD Signal vom RCCMD Sender empfangen wurde.

Eine Gruppe von 8.ncf Files können Sie in dem UPSMAN Installations Verzeichnis finden. Bitte beachten Sie, dass diese Beispiel-Files vielleicht vom Benutzer/Administrator an die Konfiguration angepasst werden müssen.

8. RCCMD auf DEC VMS

Die UPS-Management Software CD beinhaltet die RCCMD Software. Die RCCMDVMS Installation kann wie die UNIX Installation durchgeführt werden, die im Kapitel 3.2.6 in diesem Handbuch beschrieben ist.

Achtung: **Der VMS Lizenz Schlüssel ist nicht auf der Standard CD enthalten und muss separat bestellt werden.**

Sie sollten sich vor der Installation vergewissern, dass der Port 6003 nicht in Gebrauch ist. Sie können dies mit dem Befehl « netstat –an » überprüfen. Wenn Sie einen anderen Port verwenden möchten, können Sie dies mit der Option « -p » für das Senden und Empfangen starten. Beachten sie, dass Sie dann diesen Port für jeden anderen Befehl im Netzwerk verwenden müssen. Folgen Sie den Anweisungen des nächsten Kapitels sorgfältig. Nutzen Sie das Handbuch für weitere Hilfe oder kontaktieren Sie Ihren UPS Software Händler.

Wichtig: **Die Alpha Version ist zur Open VMS 7.1 verlinkt. Nutzen Sie für Open VMS 6.x die Version 6.x in dem CD-Verzeichnis VMS.ALPHA.**

Installation:

- Verbinden Sie die Workstation mit dem Netzwerk.
- Melden Sie sich am VMS System mit dem SYSTEM Login an.
- Mounten Sie das CD-ROM-Verzeichnis, wenn DKA200 der Gerätename des CD-ROM Laufwerks ist:

$ MOUNT/OVERRIDE=IDENT DKA200: UPS UPS:

Dies ist ein System spezifischer Befehl. Nutzen Sie die VMS Hilfeseiten von Ihrem System oder Fragen Sie den System Operator, wenn Sie nicht wissen, wie man mounted.

- Starten Sie die VMS Installations-Prozedur mit: @SYS$UPDATE:VMSINSTAL
- oder: @SYS$UPDATE:VMSINSTAL <device>
- z.B.: @SYS$UPDATE:VMSINSTAL RCCMD DKA200: [VMS.ALPHA]

VMSINSTAL ist ein interaktives Script. Folgen Sie einfach den Installations-Anweisungen auf dem Bildschirm (alle Anweisungen sind zusätzlich in den Subjects 5-11 aufgelistet).

- Beantworten Sie mit YES: "** Are you satisfied with the backup of your system disk [YES*]"
- Beantworten Sie: "** Where will the distribution volumes be mounted*:" with your correct input device name, z.B.:

CDROM: *dka500: [VMS]* (your CDROM device and path [VMS], the device may be different on your system).

- Beantworten Sie*:"* Enter installation options you wish to use [none]:"* by pressing RETURN
- Bei*:"Please mount the first volume of the set on MKA300:."* "** Are you ready?"* Bitte legen Sie Ihre Disk oder CD-ROM in das Laufwerk und antworten mit YES.
- Tragen Sie den Lizenz Schlüssel Ihrer RCCMD Version ein
- Tragen Sie den kompletten Pfad des Zielverzeichnisses ein, z.B: *dka100: [ups]*

- Beantworten Sie: *“Would you like to start the RCCMD module automatically on your system”.*
- Verlassen Sie die VMSINSTAL Prozedur mit RETURN bei “*Product:” prompt und bewegen Sie sich in das Zielverzeichnis (z.B.: dka100: [ups]).
- Nun installieren Sie die RCCMD Software im Sender Modus auf Ihrem RCCMD Server. Der RCCMD Server ist der Rechner, der mit der USV über den RS232-Port verbunden ist

DEC ALPHA CD Probleme: Wenn die CD nicht gemounted werden kann, oder Sie Probleme beim Starten des VMSINSTAL Scripts auf der DEC ALPHA Hardware haben, folgen Sie bitte diesen Anweisungen:

- Kopieren Sie das Archiv VMSA.ZIP (ALPHA directory) in ein temporäres Verzeichnis auf Ihrem System. COPY RCCMD.ZIP DKA100:[TEMP]

Wenn Sie kein ZIP-Programm auf Ihrer Workstation installiert haben sollten, müssen Sie einen System Wert anweisen: UNZIP==$DKA200:[VMS.ALPHA]UNZIP.EXE, wobei DKA200 Ihr CD-ROM Verzeichnis ist.

- Entpacken Sie Ihr VMS UPS Archiv:

SET DEF DKA100:[TEMP] UNZIP RCCMD.ZIP

- Starten Sie die VMS Installations Routine: @SYS$UPDATE:VMSINSTAL RCCMD DKA100:[TEMP]

Konfigurations-Prozedur:

Nach der Installation befinden sich 3 Befehls-Files auf Ihrem System:

- RCCMDSTART.COM: Der RCCMD Startbefehl sollte sich im VMS Startbefehl File befinden.
- RCCMD.COM: Befehls-File zum Starten von dem Programm, das Sie für Ihre Anforderungen entsprechend konfigurieren können.
- RCCMD_SHUTDOWN.COM: RCCMD-Befehls-File zum Herunterfahren von VMS.

Konfigurieren Sie RCCMD.COM wie folgt: “rccmd –l”, optional “rccmd –l-a (IP-Adresse des Senders)”, “-p (port, Standard ist 6003)”. Danach können Sie RCCMD mit “@rccmdstart” starten.

Prüfen Sie mit „show system“, ob ein RCCMD-Prozess vorhanden ist.

Der automatische Start von RCCMD sollte vom VMS Start-File initiiert werden. Fügen Sie folgende Zeile zu Ihrem Start-File hinzu:

$ @your_disk:[your_path]rccmdstart.com (e. g.: $ @dka100:[ups]rccmdstart.com)

Nach dem Reboot wird die UPS Software automatisch gestartet.

9. RCCMD AS400-Client

RCCMD für AS400, eine iSeries, ist in diesem Handbuch nicht beschrieben, aber hat identische Funktionen eines jeden anderen RCCMD Systems. RCCMD für AS400 wird mit einem separaten Handbuch mit dem Produkt ausgeliefert.

Download AS400 RCCMD Benutzerhandbuch

10. RCCMD FAQ

In diesem Kapitel werden bekannte Probleme mit RCCMD behandelt bzw. Hinweise für Lösungen gegeben.

FAQ – Frequently asked Questions – Fragen & Antworten

Fehler: Die Ausführung von „sudo sh rccmd_shutdow.sh“ auf ESXi 4 mit vMA 4.1 schlägt mit der folgenden oder einer ähnlichen Fehlermeldung fehl:

„Compilation failed in require at /usr/lib/perl5/site_perl/5.8.8/VMware/VIFPLib.pm line 10 BEGIN failed.“

„Compilation aborted at /usr/lib/perl5/site_perl/5.8.8/VMware/VIFPLib.pm line 10. Compilation failed in require at /usr/rccmd/upsVIShutdown.pl line 12.“

„Can't load '/usr/lib/perl5/site_perl/5.8.8/libvmatargetlib_perl.so' for module vmatargetlib_perl: libtypes.so: cannot open shared object file: No such file or directory at /usr/lib64/perl5/5.8.8/x86_64-linux-thread-multi/DynaLoader.pm line 230.“

„BEGIN failed--compilation aborted at /usr/rccmd/upsVIShutdown.pl line 12. at /usr/lib/perl5/site_perl/5.8.8/VMware/VmaTargetLib.pm line 10.“

Ursache: Sie versuchen eine RCCMD Version für die vMA 4.0 zu installieren, welche auf vMA 4.1 oder höher zu diesem Fehler führt.

Lösung: Die RCCMD Version für die vMA 4.1 oder höher verwenden.

Problem: Sie erhalten folgende Fehlermeldung bei der Ausführung der upsVIShutdown.pl:

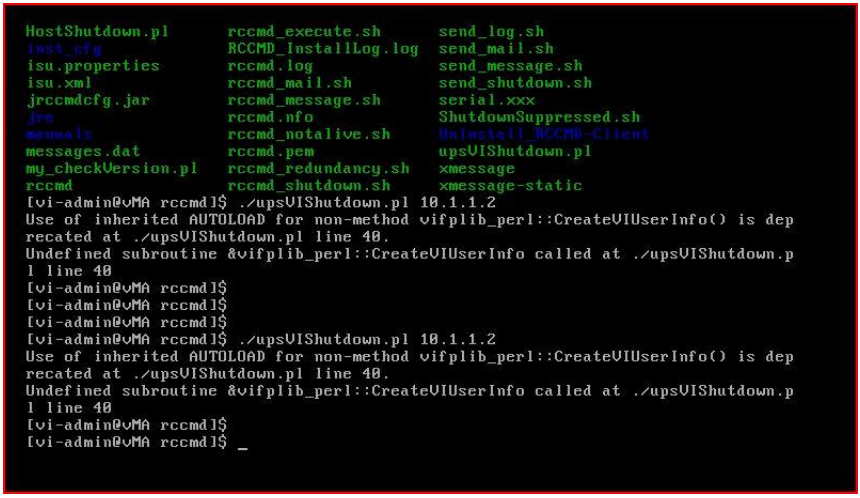

Abb. 236: Fehlermeldung nach Ausführung der upsVIShutdown.pl

Lösung: Sie verwenden nicht die aktuellste RCCMD Version. Bitte laden Sie das neueste Download-Paket von unserer Webseite www.generex.de herunter.

Problem: Shutdown von NetApp Storages

Lösung: Generell exportieren alle NAS Systeme Ihre NFS Shares im "Async" Modus. Dies ist ein extrem schneller Schreibprozess, der gewährleistet, dass bei einem plötzlichen Stromausfall kein Datenverlust entsteht. Solange der Anwender den Standard NFS Protokoll Schreibmodus nicht von "Async" auf "Sync" verändert hat, besteht kein Risiko, Daten zu verlieren.

Dennoch sollte eine USV an jedes NAS angeschlossen werden, um den Fall abzusichern, dass Netzwerkcomputer NICHT heruntergefahren werden, sondern einfach "ausgehen".Für diesen Fall ist eine USV am NAS notwendig, und dafür finden wir es auch sinnvoll, an ein NAS System eine USV anzuschliessen.

Ansonsten ist es ausreichend, wenn die Rechner im Netzwerk bei einem Stromausfall (per RCCMD) heruntergefahren werden. Wenn die Rechner angehalten sind, gibt es auch keine offenen Dateien mehr, die verloren gehen können. Sie könnten also jedes NAS einfach ausschalten, sobald die Rechner im Netzwerk angehalten sind. Das NAS kann dann einfach abgeschaltet werden.

Besonderheit: QNAP/NetApp Systeme verwenden den "Sync" Modus, sind damit schneller und damit entsprechend empfindlicher. Aber diese Geräte besitzen eine eigene Batterie, um einen sicheren Shutdown immer gewährleisten zu können. Dieser interne Akku leert den Cache und parkt die Schreibköpfe, wenn keine Daten zu speichern sind. Auch hier gilt, dass man keine Daten verliert, wenn die Rechner angehalten wurden.

Eine zusätzliche Verbindung der USV und NAS mittels eines USB Kabels oder Shutdownsignals über

Netzwerk halten wir für nicht notwendig, wenn vorher sichergestellt wurde, dass die Rechner angehalten wurden.

Problem: Fehlermeldungen bei „UPSMAN Alive Check“ auf Windws Server 2008

Lösung: Der Firewall Port 5769 muss für alle Profile (Domäne, Heim, öffentlich) freigeschaltet werden!

Problem: Mounten eines USB-Sticks via Kommndozeile

Lösung: Wechseln Sie in das Verzeichnis /dev. Führen Sie ls aus. Dort befinden sich die angeschlossenen Geräte. Merken Sie sich, was bei Ihnen bei sda, sda1... aufgeführt ist. Schliessen Sie den USB-Stick an den Server an. Führen Sie erneut im Verzeichnis /dev ls aus. Nun sollten sich unter sda mehrere Einträge finden. Auf meinem Server heisst mein Stick sdc1. Geben Sie Folgendes ein: mount /dev/*sdc1* /mnt
Auf **FreeBSD** lautet das Kommando: mount_msdosfs /dev/da0s1 /mnt/usb

Führen Sie ls -lisa aus.
Nun sollten Sie die vorhandenen Verzeichnisse auf Ihrem Stick sehen können.
Wechseln Sie in das entsprechende Verzeichnis mit: cd /mnt/Name des entsprechenden Verzeichnisses, in dem sich die Installationsdateien befinden. Extrahieren Sie das rccmdinst.tar File mit: tar -xvf rccmdinst.tar
Führen Sie die Binärdatei aus mit: ./installRCCMD.bin

Problem: Die RCCMD Software führt keine Shutdowns aus, und Sie erkennen folgende Fehlermeldung in der Datei „rccmd.log“ (Standard Verzeichnis C:\Program Files\RCCMD):

11/23/2011,12:56:55, RCCMD: ERR: WaitForOkay - Read failed with error <0>

Lösung: Updaten Sie Ihre RCCMD Software!

Problem: Sie erhalten folgende Meldung im CS121 AlarmLog:

```
12/06/2011,16:30:56, RCCMD could not connect. (RccmdConn01) Reason: Host prohibited
```

Lösung: Der angegebene Server lehnt eine eingehende TCP-Verbindung ab. Überprüfen Sie Ihre Firewall Konfiguration.

Problem: Prüfen der Firewall Ports auf UNIX OS

Lösung: Ob die Ports 6003 und 5769 wirklich offen sind, sehen Sie mit:

```
sudo iptables –L
```

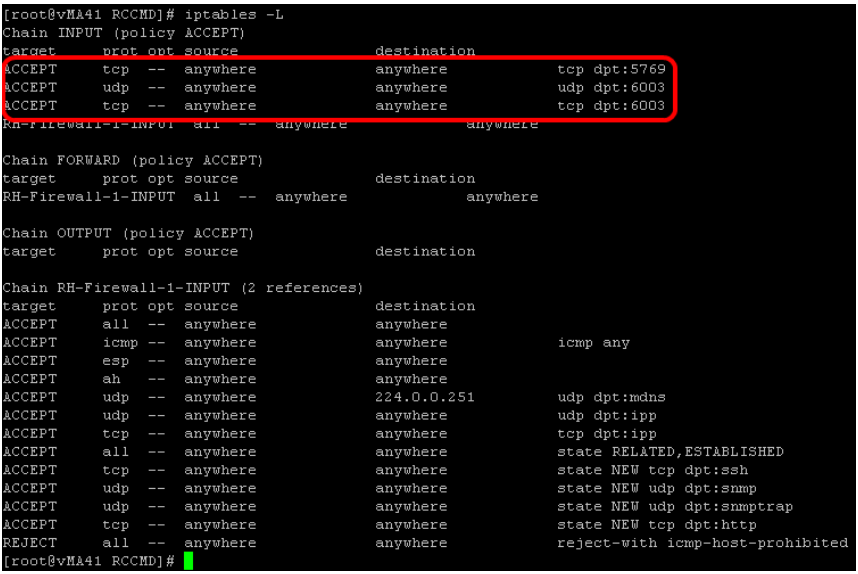
[root@vMA41 RCCMD]# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT tcp -- anywhere anywhere tcp dpt:5769
ACCEPT udp -- anywhere anywhere udp dpt:6003
ACCEPT tcp -- anywhere anywhere tcp dpt:6003
RH-Firewall-1-INPUT all -- anywhere anywhere
Chain FORWARD (policy ACCEPT)
target prot opt source destination
RH-Firewall-1-INPUT all -- anywhere anywhere
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain RH-Firewall-1-INPUT (2 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere
ACCEPT icmp -- anywhere anywhere icmp any
ACCEPT esp -- anywhere anywhere
ACCEPT ah -- anywhere anywhere
ACCEPT udp -- anywhere 224.0.0.251 udp dpt:mdns
ACCEPT udp -- anywhere anywhere udp dpt:ipp
ACCEPT tcp -- anywhere anywhere tcp dpt:ipp
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh
ACCEPT udp -- anywhere anywhere state NEW udp dpt:snmp
ACCEPT udp -- anywhere anywhere state NEW udp dpt:snmptrap
ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:http
REJECT all -- anywhere anywhere reject-with icmp-host-prohibited
[root@vMA41 RCCMD]#

Abb. 237: Auflistung IP-Tables, man sieht am „ACCEPT“ das TCP und UDP Port 6003 offen sind, weiterhin TCP Port 5769

Sollte das Installscript die Ports nicht öffnen können, so ist dies auch manuell möglich:

Manuelles Freischalten der Firewall Ports 6003 UDP/TCP

Sie können wie folgt den Port 6003 UDP/TCP freischalten:

```
/usr/sbin/esxcfg-firewall

esxcfg-firewall -o 6003,tcp,in,"RCCMD receive 6003"
esxcfg-firewall -o 6003,udp,in,"RCCMD receive udp 6003"
esxcfg-firewall -o 6003,tcp,out,"RCCMD transmit 6003"
esxcfg-firewall -o 6003,udp,out,"RCCMD transmit udp 6003"

oder

/usr/sbin/iptables oder /sbin/iptables

iptables -I INPUT -p tcp --dport 6003 -j ACCEPT
iptables -I OUTPUT -p tcp --sport 6003 -j ACCEPT
iptables -I INPUT -p udp --dport 6003 -j ACCEPT
iptables -I OUTPUT -p udp --sport 6003 -j ACCEPT
```

Speichern Sie die Einstellungen mit:

```
service iptable save
```

Problem: RCCMD Fehlermeldung auf VMware ESXi Server:

04/25/2012,14:40:24, rccmd[08066]: message received from 192.168.2.67

04/25/2012,14:40:24, rccmd[08066]: Trying to start program/job: /usr/rccmd/rccmd_shutdown.sh

04/25/2012,14:40:24, rccmd[08066]: error: /usr/rccmd/rccmd_shutdown.sh program/**job start failed**

Der Fehler "job start failed" erscheint, wenn der User keine Berechtigung für das Ausführen der rccmd_shutdown.sh hat.

Lösung 1: Es muss ein X für die rccmd_shutdown.sh wie folgt eingerichtet werden:

```
CHMOD +x rccmd_shutdown.sh
```

Lösung 2: Wenn die Berechtigungen für die rccmd_shutdown.sh vorhanden sind, wurden während der Installation inkorrekte Angaben bei den ESXi Server Login-Daten gegeben. Diese können in der Datei "esxi_creds" im Verzeichnis /usr/rccmd korrigiert werden.

Problem: Sie erhalten nach dem Start der Installation auf einer vMA auf einem ESXi Server folgende Meldung:

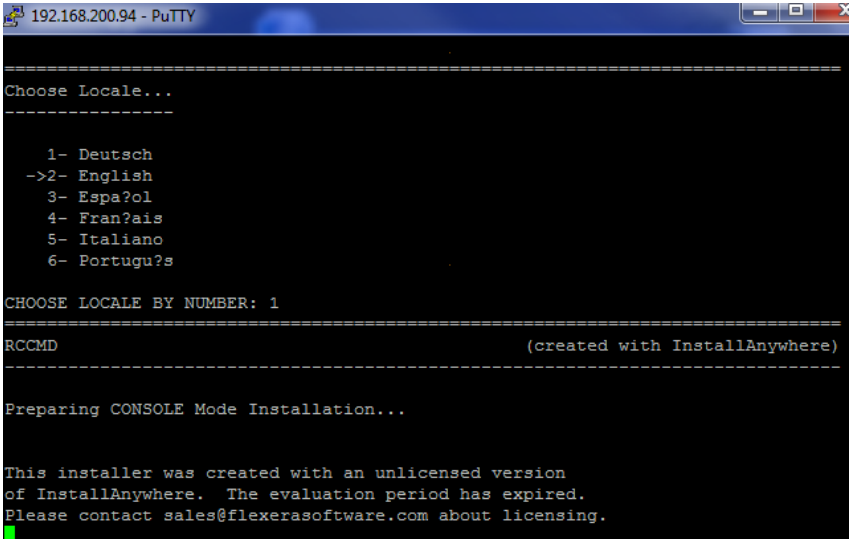

Abb. 238: Fehlermeldung „Unlicensed Version"

Lösung 1: Um RCCMD auf einer vMA installieren zu können, ist es erforderlich, dass auf dem OS ein TMP-Verzeichnis (/tmp) vorhanden ist.

Appendix

A OpenSSL

"This product includes software developed by the OpenSSL Project for use

in the OpenSSL Toolkit (http://www.openssl.org/).

B Syntax zum Schalten von Ausgängen

Den RCCMD Empfänger auf Port 6002 auf „On“ stellen, die AUX-Ports des CS121 als Outputs definieren und neu starten. Installieren Sie den RCCMD Windows Wizard, und öffnen Sie eine DOS-Box. Es folgt ein Syntax-Beispiel mit der IP-Adresse 192.168.202.165:

```
C:\Program Files\RCCMD\

rccmd -se "EXECUTE |AUX|1|1" -a 192.168.202.165 -p 6002
```

ACHTUNG! Die Leerzeile nach dem EXECUTE ist wichtig!

Allgemeine Syntax für das Schalten von AUX Ports:

```
|AUX|1|0  Port1, auf low setzen
|AUX|1|1  Port1, auf high setzen
|AUX|2|0  Port2, auf low setzen
|AUX|2|1  Port2, auf high setzen
|AUX|3|0  Port3, auf low setzen
|AUX|3|1  Port3, auf high setzen
|AUX|4|0  Port4, auf low setzen
|AUX|4|1  Port4, auf high setzen
```

Syntax-Beispiel für das Schalten der Outputs am SiteManager:

```
C:\Program Files\RCCMD\rccmd -s -a 192.168.222.238 -p 6002 -se "EXECUTE
|UPSCMD|20000|1,1"
```

ACHTUNG! Die Leerzeile nach dem EXECUTE ist wichtig!

```
|UPSCMD|20000|1,0  Ausgang 1 auf low
|UPSCMD|20000|1,1  Ausgang 1 auf high
|UPSCMD|20000|2,0  Ausgang 2 auf low
|UPSCMD|20000|2,1  Ausgang 2 auf high
|UPSCMD|20000|3,0  Ausgang 3 auf low
|UPSCMD|20000|3,1  Ausgang 3 auf high
|UPSCMD|20000|4,0  Ausgang 4 auf low
|UPSCMD|20000|4,1  Ausgang 4 auf high
|UPSCMD|20000|5,0  Ausgang 5 auf low
|UPSCMD|20000|5,1  Ausgang 5 auf high
|UPSCMD|20000|6,0  Ausgang 6 auf low
|UPSCMD|20000|6,1  Ausgang 6 auf high
```

```
|UPSCMD|20000|7,0  Ausgang 7 auf low
|UPSCMD|20000|7,1  Ausgang 7 auf high
|UPSCMD|20000|8,0  Ausgang 8 auf low
|UPSCMD|20000|8,1  Ausgang 8 auf high
```

C Know How Pool

SuSE 8.1 und ältere Linux Versionen

Wenn Sie SuSE 8.1 oder eine ältere Linux Version nutzen, müssen Sie während der interaktiven RCCMD Installation als OS „XEN-Server“ auswählen!

D RARITAN Dominion PDU Konfiguration

Im folgenden Abschnitt beschreiben wir, wie ein RARITAN PDU Typ Dominion durch einen RCCMD Client, CS121 oder jedem anderen RCCMD kompatiblen Gerät gesteuert werden kann:

1. Installieren Sie RCCMD auf einem Windows OS, und kopieren/erstellen Sie ein Batch-File, wie das folgende, in das RCCMD Verzeichnis (Standard: C:\Program Files\RCCMD), und verwenden Sie ein SNMPwalk Tool von einer Open Source mit der obligatorischen Auslieferungs-Datei “Copying.txt”. Diese Datei ist gesetzlich zulässig enthalten (Open Source).

```
@echo off
set PX_OID=1.3.6.1.4.1.13742.4.1.2.2.1.3.

if x%1==x goto paramerror
if x%2==x goto paramerror
if x%3==x goto paramerror
if x%4==x goto paramerror

snmpset -v 2c -c %2 %1 %PX_OID%%3 i %4
goto end

:paramerror
echo.
echo missing parameter!
echo.
echo Usage: pxout.bat ip community port value
echo ip:        address of the PX device
echo community: SNMP community string
echo port:      1-12
echo value:     0 or 1

:end
```

Abb. 239: „pxout.bat“

Das Batch-File wurde “pxout.bat” genannt und erwartet 4 Parameter:

- IP-Adresse oder Hostname vom Raritan Gerät
- SNMP Community String (mit Write Access)
- Outlet Nummer (1 bis 12)
- 0 = aus, 1 = an

2. Das Batch-File “pxout.bat” akzeptiert nun mehrere Parameter von eingehenden RCCMD Kommandos und übersetzt diese in SNMP Set Commands für das Raritan.

Das “pxout.bat” akzeptiert die folgende Syntax:

“pxout.bat” <IP-Adresse> <Community> <Outlet> <an/aus>

- **IP-Adresse**: Die IP-Adresse des Raritan

- **Community**: Der Community String für “Write Access”, konfiguriert auf dem Raritan oder SNMP Set Commands, Standard ist “public”
- **Outlet**: Die Nummer des Raritan Outlet von 1 bis 12, der geschaltet werden soll
- **An/Aus**: Das Signal, dass Sie übertragen möchten, “0” ist aus, “1” ist an
- Beispiel: “pxout.bat 192.168.200.11 public 0” dieses Beispiel wird das Raritan Gerät mit der IP-Adresse 192.168.200.11 das Outlet 4 ausschalten.

Wenn dies manuell von Ihrem Windows/RCCMD PC manuell funktioniert, können Sie mit Schritt 3 fortfahren.

3. Wählen Sie nun einen gewünschten CS121 Event, und fügen ie ein RCCMD Kommando hinzu, welches zu dem Windows PC gesendet wird, wo RCCMD läuft und die “pxout.bat” Datei liegt.

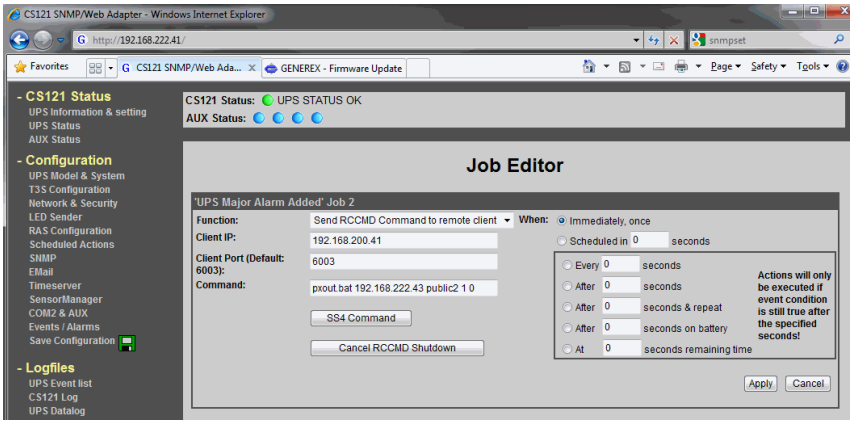

Abb. 240: CS121 Konfiguration von einem Relay-Kommando

Das Ziel von dem RCCMD Kommando ist der Windows PC mit RCCMD und der “pxout.bat” mit der IP-Adresse 192.168.200.41. Wenn der Event “UPS Major Alarm Added” auftritt, wird dieser Job das Kommando “pxout.bat 192.168.222.43 public2 1 0” sofort ausführen, um den Outlet Nummer 4 auf dem Raritan mit der IP-Adresse 192.168.222.43 auszuschalten.

Tipp: Sie sollten RCCMD als Hintergrundprozess auf diesem Windows PC stoppen, um besser erkennen zu können, was passiert. Stoppen Sie den RCCMD Dienst, öffnen Sie eine Kommando-Zeile in dem RCCMD Verzeichnis, und starten Sie “rccmd.exe –debug”. Die Software läuft nun im Vordergrund, und Sie können die Kommunikation beobachten.

4. Das Raritan Gerät mit der FirmWare 1.4.1 ist leider buggy. Hier ist der Workaround:

Der Standard Community String für das Raritan ist identisch gesetzt auf “read” und “write” zu “public”, aber diese Konfiguration ist falsch! Es müsste anders sein.

Lösung: Stoppen Sie den SNMP Agent auf dem Raritan, ändern Sie die Community für “write” auf jede andere als “public”, und starten Sie den Dienst neu!

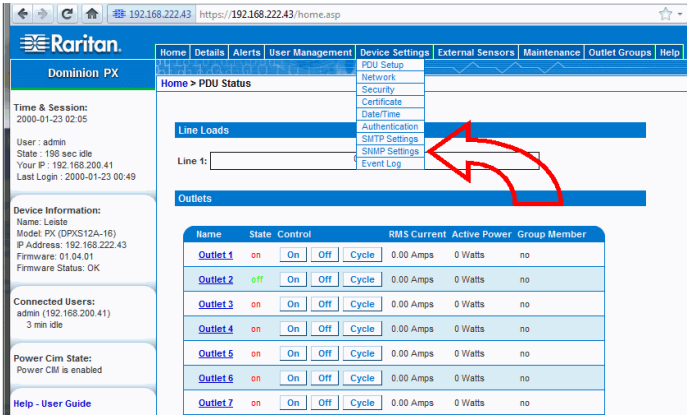

Abb. 241: Raritan Device Settings

Der Standard Raritan User ist „admin, Passwort „nimda“.

Achtung! Dies funktioniert nicht mit dem MS Internet Explorer! Verwenden Sie jeden anderen Webbrowser, z. B. Mozilla Firefox.

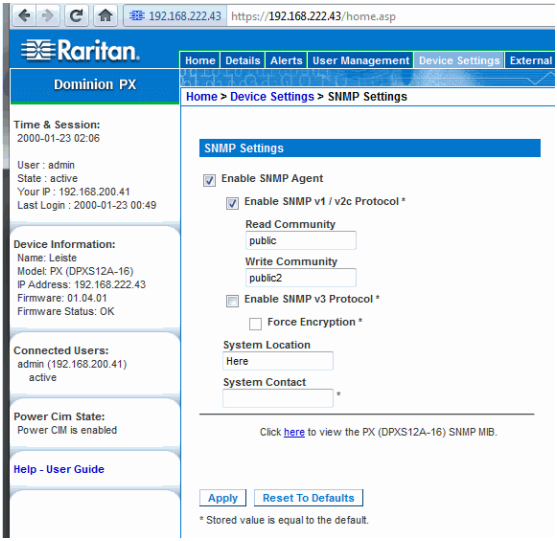

Abb. 242: Raritan SNMP Settings

Klicken Sie auf « Stop », ändern Sie die Konfiguration für « Write Community », z. B. auf « public2 », und starten Sie neu!

E Abbildungen

Abb. 1: RCCMD und UPSMAN in einer Netzwerkumgebung 7
Abb. 2: Einführung 8
Abb. 3: Lizenzschlüssel Eintrag 9
Abb. 4: Lizenzvertrag 9
Abb. 5: Installationssatz Auswahl 10
Abb. 6: Installationsordner Auswahl 10
Abb. 7: Firewall Ausnahmen 11
Abb. 8: RCCMD Tray 11
Abb. 9: Auswahl Verknüpfungsordner 12
Abb. 10: Prä-Installations Übersicht 12
Abb. 11: WebIf Zugriff einstellen 13
Abb. 12: Kennworteingabe 13
Abb. 13: Passworthinweis-Eingabe 14
Abb. 14: Installations Abschluss 14
Abb. 13: Dateiinhalt „installer.properties“ 17
Abb. 15: RCCMD Console Installation – Sprachauswahl, Einführung 19
Abb. 16: RCCMD Console Installation – Eingabe Lizenzschlüssel, Lizenzvertrag 19
Abb. 20: RCCMD Configurator 21
Abb. 21: RCCMD Configurator 22
Abb. 22: RCCMD WebInterface Configurator – Connections 23
Abb. 23: RCCMD WebInterface Configurator – Heartbeats 24
Abb. 24: RCCMD WebInterface Configurator – Redundancy 25
Abb. 25: RCCMD WebInterface Configurator – Shutdown Settings 27
Abb. 26: RCCMD WebInterface Configurator – Shutdown Settings – Edit File 27
Abb. 27: RCCMD WebInterface Configurator – E-mail Settings 28
Abb. 28: RCCMD WebInterface Configurator – Notification Settings 29
Abb. 29: RCCMD WebInterface Configurator – Advanced Settings 30

Abb. 30: RCCMD WebInterface Configurator – Web Configuration 31
Abb. 31: RCCMD WebInterface Configurator – User Settings 31
Abb. 32: RCCMD WebInterface Configurator – View Event Log 32
Abb. 33: RCCMD WebInterface Configurator – System Status 33
Abb. 34: RCCMD WebInterface Configurator – Help 33
Abb. 35: RCCMD WebInterface Configurator – Remote Zugriff 34
Abb. 36: Example: Batch File RCCMD als Relay Station 35
Abb. 37: CS121 Konfiguration „WAKEUP“ Befehl 36
Abb. 38: UPSMAN Konfiguration „WAKEUP“ Befehl 36
Abb. 39: „WAKEUP“ Befehl im RCCMD Log 37
Abb. 40: RCCMD SSL Einstellung 37
Abb. 41: Timeserver Konfiguration 38
Abb. 42: Speichern der Einstellungen 38
Abb. 43: SSL Konfiguration 39
Abb. 44: RCCMD Eigenschaften Fenster 40
Abb. 45: RCCMD Eigenschaften Log On Fenster 41
Abb. 46: RCCMD Eigenschaften Passwort-Bestätigung 41
Abb. 47: Select User Fenster 42
Abb. 48: Auswahl des Objektnamens 42
Abb. 49: Administrator Auswahl 43
Abb. 50: Administrator Passwort Bestätigung 43
Abb. 52: System Status – Restart RCCMD 45
Abb. 53: RCCMD Konsolen-Test 46
Abb. 54: RCCMD Alive Check via Befehlszeile 46
Abb. 55: RCCMD Konsole -? 47
Abb. 56: RCCMD Konfiguration 50
Abb. 57: Client Installation 50
Abb. 58: Eingabe IP-Adresse 51
Abb. 59: Erweiterte Netzwerk Einstellungen 51

Abb. 60: UPSMAN Alive Checking / Redundanz Fenster 52
Abb. 61: Client Check Connection Batch File Fenster 53
Abb. 62: Check UPSMAN Connections Fenster 54
Abb. 63: Konfiguration der Batch Files Fenster 54
Abb. 64: RCCMD Log File 55
Abb. 65: RCCMD Email Settings 55
Abb. 66: CS121 Email Kommando 56
Abb. 67: RCCMD Shutdown Sequenz Konfiguration 56
Abb. 68: Example: Batch File RCCMD als Relay Station 57
Abb. 69: RCCMD Client Shutdown Konfiguration 57
Abb. 70: RCCMD Shutdown Relay 58
Abb. 71: RCCMD Konfiguration IP-Adressen-Bereich 58
Abb. 72: RCCMD Shutdown Relay Adress-Entfernung 59
Abb. 73: RCCMD Shutdown Relay in der „Shutdwown.bat“ 59
Abb. 74: Installation – Einführung 61
Abb. 75: Installation – Lizenzeingabe 61
Abb. 76: Installation – Installationssatz Auswahl 62
Abb. 77: Installation – Ordnerauswahl 62
Abb. 78: Installation – Auswahl der Wiedergabemöglichkeiten 63
Abb. 79: Installation – Prä-Installations-Übersicht 63
Abb. 80: Installation – Auswahl RCCMD WebIf Zugriff 64
Abb. 82: Installation – Kennworteingabe 65
Abb. 83: Installation – Passworthinweis-Eingabe 65
Abb. 85 Installation – RCCMD Start Hinweis 66
Abb. 86: Installation – Abschluss 67
Abb. 87: Console Installation – Sprachauswahl, Einführung 70
Abb. 88: Console Installation – OS/Plattform Erkennung, Lizenzeingabe, Lizenzvertrag 71
Abb. 89: Console Installation – Produktfunktions-Auswahl, Übersicht 71
Abb. 90: Console Installation – Autostart 72

Abb. 91: Console Installation – Weblf Auswahl 72
Abb. 92: Console Installation – Hinweis, Firewall Ausnahme 72
Abb. 93: Console Installation – RCCMD Start, Installations-Abschluss 73
Abb. 94: RCCMD WebInterface 73
Abb. 95: RCCMD WebInterface – Connections 74
Abb. 96: RCCMD WebInterface – Heartbeats 75
Abb. 97: RCCMD WebInterface – Redundancy 76
Abb. 98: RCCMD WebInterface – Shutdown Settings 77
Abb. 99: RCCMD WebInterface – Notification Settings 77
Abb. 100: RCCMD WebInterface – Advanced Settings 78
Abb. 101: RCCMD WebInterface – Web Access 79
Abb. 102: RCCMD WebInterface – User Settings 79
Abb. 103: RCCMD WebInterface – Event Log 80
Abb. 104: RCCMD WebInterface – System Status 80
Abb. 105: RCCMD WebInterface – Help 81
Abb. 106: RCCMD WebInterface – Remote Zugriff 81
Abb. 107: CS121 Konfiguration „WAKEUP“ Befehl 82
Abb. 108: UPSMAN Konfiguration „WAKEUP“ Befehl 83
Abb. 110: RCCMD SSL Konfiguration 84
Abb. 111: Timeserver Konfiguration 84
Abb. 112: Speichern der Einstellungen 85
Abb. 113: SSL Konfiguration 85
Abb. 114: Konfiguration – IP-Adressen Fenster 89
Abb. 115: Konfiguration – Functions 90
Abb. 116: Konfiguration – RCCMD Redundanz 91
Abb. 117: Konfiguration – RCCMD Log File 92
Abb. 118: Konfiguration – RCCMD Execute 92
Abb. 119: Konfiguration – RCCMD Configure Email 93
Abb. 120: Konfiguration – RCCMD Shutdown.sh 93

Abb. 121: Konfiguration – RCCMD Shutdown Sequenz 94
Abb. 123: Konfiguration – RCCMD Shutdown.sh 95
Abb. 124: Konfiguration – RCCMD Shutdown Sequenz 96
Abb. 125: Konfiguration – RCCMD Relay Konfiguration IP-Adressen-Bereich 96
Abb. 126: Erstellung des Konfigurations-Files 97
Abb. 127: RCCMD Konfigurations-Menü UNIX 98
Abb. 128: RCCMD UNIX Netzwerk Optionen 99
Abb. 129: Hinzufügen RCCMD UNIX Sender 101
Abb. 130: RCCMD UNIX Sender Beispiel 101
Abb. 131: RCCMD UNIX Sender Überblick 102
Abb. 132: RCCMD UNIX Sender Editierung 102
Abb. 133: RCCMD UNIX Sender Löschen 103
Abb. 134: RCCMD UNIX Sender Scan 104
Abb. 135: RCCMD UNIX Check Upsman 105
Abb. 136: RCCMD UNIX Log File Optionen 106
Abb. 137: RCCMD UNIX Shutdown Optionen 107
Abb. 138: RCCMD UNIX File Browsing 108
Abb. 139: vSphere-Client Konfiguration 113
Abb. 140: vSphere-Client Autostart-Konfiguration 113
Abb. 141: vSphere-Client- Autostart-Verzögerung 114
Abb. 142: vSphere-Client – Startup and Shutdown 114
Abb. 143: Installationsvorbereitung 116
Abb. 144: Ausführung der Binärdatei installRCCMD.bin und Beginn des Installationsskriptes 116
Abb. 145: Sprachauswahl und Beginn der Installation - die Meldung „Recognized VMware ESXi environment“ zeigt an, dass die richtige Hardware erkannt wurde 117
Abb. 146: Lizenz Eingabe 117
Abb. 147: Produkt Feature Auswahl 118
Abb. 148: Interaktive Eingaben – vCenter, ESXi Server Hostname oder IP-Adresse 118
Abb. 149: Interaktive Eingaben – Herunterfahrzeit, vMA Name 119

Abb. 150: Interaktive Eingaben – vCenter Zugangsdaten 119
Abb. 151: Interaktive Eingaben – Installationsübersicht 120
Abb. 152: Interaktive Eingaben – Portauswahl, Passworteingabe 120
Abb. 153: Interaktive Eingaben – Hinweis, Abschluss 121
Abb. 155: Installer meldet das Firewall Port 6003 und 5769 geöffnet wurden 122
Abb. 157: RCCMD WebInterface – Remote Zugriff 123
Abb. 158: RCCMD WebInterface – RCCMD im vCenter 123
Abb. 159: RCCMD WebInterface – Connections 124
Abb. 160: RCCMD WebInterface – Heartbeats 125
Abb. 161: RCCMD WebInterface – Redundancy 126
Abb. 162: RCCMD WebInterface – vMA Shutdown Settings 127
Abb. 163: RCCMD WebInterface – Notification Settings 128
Abb. 164: RCCMD WebInterface – Remote Zugriff – VMware Settings 128
Abb. 166: RCCMD WebInterface – VMware Settings – vMA Name 130
Abb. 167: RCCMD WebInterface – Advanced Settings 131
Abb. 168: RCCMD WebInterface – Web Access 132
Abb. 169: RCCMD WebInterface – User Settings 132
Abb. 170: RCCMD WebInterface – Event Log 133
Abb. 171: RCCMD WebInterface – System Status 133
Abb. 172: RCCMD WebInterface – Help 134
Abb. 173: Installationsvorbereitung 135
Abb. 174: Ausführung der Binärdatei installRCCMD.bin und Beginn des Installationsskriptes 135
Abb. 175: Sprachauswahl und Beginn der Installation - die Meldung „Recognized VMware ESXi environment“ zeigt an, dass die richtige Hardware erkannt wurde 136
Abb. 176: Lizenz Eingabe 136
Abb. 177: Produkt Feature Auswahl 137
Abb. 178: Interaktive Eingaben – vCenter, ESXi Server Hostname oder IP-Adresse 137
Abb. 179: Interaktive Eingaben – Herunterfahrzeit, vMA Name 138
Abb. 180: Interaktive Eingaben – vCenter Zugangsdaten 138

Abb. 181: Interaktive Eingaben – Installationsübersicht 139
Abb. 184: RCCMD WebInterface – Remote Zugriff 141
Abb. 185: RCCMD WebInterface – Connections 141
Abb. 186: RCCMD WebInterface – Heartbeats 142
Abb. 187: RCCMD WebInterface – Redundancy 143
Abb. 188: RCCMD WebInterface – vMA Shutdown Settings 144
Abb. 189: RCCMD WebInterface – Notification Settings 145
Abb. 190: RCCMD WebInterface – Remote Zugriff – VMware Settings 146
Abb. 192: vSphere Web Client, RCCMD WebInterface – VMware Settings – vMA Name 148
Abb. 193: RCCMD WebInterface – Advanced Settings 149
Abb. 194: RCCMD WebInterface – Web Access 150
Abb. 195: RCCMD WebInterface – User Settings 150
Abb. 196: RCCMD WebInterface – Event Log 151
Abb. 197: RCCMD WebInterface – System Status 151
Abb. 198: RCCMD WebInterface – Help 152
Abb. 199: Firewall Konfiguration 155
Abb. 200: RCCMD Installation-Einführung 156
Abb. 201: RCCMD Lizenz Schlüssel Eingabe 157
Abb. 202: RCCMD Installationssatz Auswahl 157
Abb. 203: RCCMD Aliasordner Auswahl 158
Abb. 204: RCCMD Nachrichten 158
Abb. 205: Prä-Installations-Übersicht 159
Abb. 206: WebIf Zugriff einstellen 159
Abb. 207: Kennworteingabe 160
Abb. 208: Passworthinweis-Eingabe 160
Abb. 209: RCCMD Konfiguration erforderlich 161
Abb. 210: Installationssabschluss 161
Abb. 211: RCCMD WebInterface 162
Abb. 212: RCCMD WebInterface – Connections 162

Abb. 213: RCCMD WebInterface – Heartbeats 163
Abb. 214: RCCMD WebInterface – Redundancy 164
Abb. 215: RCCMD WebInterface – Shutdown Settings 165
Abb. 216: RCCMD WebInterface – Notification Settings 166
Abb. 217: RCCMD WebInterface – Advanced Settings 166
Abb. 218: RCCMD WebInterface – Web Access 167
Abb. 219: RCCMD WebInterface – User Settings 168
Abb. 220: RCCMD WebInterface – Event Log 168
Abb. 222: RCCMD WebInterface – System Status 169
Abb. 223: RCCMD WebInterface – Help 169
Abb. 224: RCCMD WebInterface – Remote Zugriff 170
Abb. 226: RCCMD IP Adressen Fenster 170
Abb. 227: RCCMD Konfigurations-Fenster „Functions“ 171
Abb. 228: RCCMD Check UPSMAN Verbindungen 172
Abb. 229: RCCMD Redundanz 172
Abb. 230: RCCMD Konfigurations-Fenster „Logfile“ 173
Abb. 231: RCCMD Konfigurations-Fenster „Execute“ 173
Abb. 232: RCCMD E-Mail-Konfiguration 174
Abb. 233: Konfiguration – RCCMD Shutdown.sh 174
Abb. 234: Konfiguration – RCCMD Shutdown Sequenz 175
Abb. 235: RCCMD Control 175
Abb. 236: Fehlermeldung nach Ausführung der upsVIShutdown.pl 183
Abb. 237: Auflistung IP-Tables, man sieht am „ACCEPT“ das TCP und UDP Port 6003 offen sind, weiterhin TCP Port 5769 185
Abb. 239: „pxout.bat“ 188
Abb. 240: CS121 Konfiguration von einem Relay-Kommando 189
Abb. 241: Raritan Device Settings 190
Abb. 242: Raritan SNMP Settings 190